opentext™

ZENworks
Patch Management Reference

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

© Copyright 2008 - 2024 Open Text

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Open Text”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide 7

1 Patch Management Overview 9

What's New . . . 9
Product Overview . . . 9
Supported Environments and Patch Content . . . 10
Patch Management Process and Workflow . . . 11

2 Post Migration Tasks 13

Enabling Native Update Channel Patching . . . 13
SUSE and Red Hat Patching . . . 13
Enable Microsoft 365 Apps Patching . . . 14
Enabling Software Installers . . . 14
Enable Software Installers at the Zone Level . . . 15
Enable Software Installers at the Device Folder Level . . . 15
Enable Software Installers for an Individual Device . . . 15
Enabling Firewall Access to Patch Vendor URLs . . . 15

3 Configure Patch Management 17

Activating Patch Management . . . 17
Starting the Patch Service . . . 21
Configuring the Patch Server . . . 21
Patch Server . . . 21
Maintenance Schedule . . . 21
Reset ZENworks Patch Management . . . 22
Ondemand Content Master - Requirements . . . 22
Configuring the CVE Subscription . . . 23
Configuring Patch Pre-Fetch Settings . . . 23
Pre-Fetch Actions . . . 24
Languages . . . 24
Configuring Pre-Cached Content . . . 24
Content Types . . . 24
Content Servers . . . 25
Overriding Zone Pre-Cached Settings . . . 25
Cleaning up Patch Content . . . 25
Configuring the Security Dashboard . . . 28
Configuring Email Notification . . . 28
Configuring the Schedule for Vulnerability Detections . . . 29
Setting Vulnerability Detection at the Folder Level . . . 32
Initiating a Patch Scan . . . 33
Scan using updated patch scan signature (DAU) file . . . 33
Scan using device's current patch scan signature (DAU) file . . . 33
No scan; retrieve existing scan results only . . . 33
Configuring Patch Policy Settings . . . 33

Schedule Enforcement . . . 34
Patch Policy Reboot Behavior . . . 36
Configure Patch Policy Settings at the Folder Level . . . 37
Configuring Patch Policy Pre-Install Behavior . . . 37
Schedule Distribution . . . 37
Pre-Install Notification Options . . . 39
Configure Patch Policy Pre-Install Behavior at the Folder Level . . . 40

4 Assess Vulnerabilities 41

Security Pages . . . 41
Employing the Security and Patch Dashboard . . . 41
Viewing Patch Policies . . . 48
Viewing Zone Patches . . . 48
Viewing Patch Status . . . 49
Viewing Patches for a Device . . . 50
Accessing Patch Management Reports . . . 53
Viewing Predefined Reports . . . 53
Generating Patch Audit Reports . . . 54
Common Patch Management Reports . . . 55

5 Distribute and Apply Patches 57

Understanding Pre-Fetching and Pre-Caching of Patches . . . 57
Creating and Publishing Patch Policies . . . 58
Patch Policy - Best Practices . . . 58
Create a Patch Policy . . . 60
Editing Patch Policies . . . 65
Assign a Patch Policy to Devices . . . 65
Test a Policy Before Deploying to a Live Environment . . . 66
Configuring the Success Rate for Patch Test Devices . . . 67
Publish a Patch Policy . . . 67
Deploying Patches Manually . . . 68
Create a Deployment Schedule . . . 68
Confirm Devices . . . 69
Remediation Schedule . . . 70
Deployment Order and Behavior . . . 74
Remediation Options . . . 75
Pre-Install Notification Options . . . 75
Distribution Schedule . . . 76
Notification and Reboot Options . . . 79
Choose Deployment Name . . . 81
Deployment Summary . . . 82
Deploying Patches on Mac Devices . . . 82
Applying Patches to Intel Devices . . . 82
Applying Patches to ARM Devices . . . 83

6 Best Practices 85

Testing Patches . . . 86
Deploying Patches in a Controlled Way . . . 86
Monitoring Patch Implementation . . . 86
Tuning the Patch Management Service . . . 87

Tuning the Patch Management Microservice 87

7 Manage Patches 93

Configure the Patch Display 93
View Patch Details. 94
Zone-Level Patches 94
Device Patches 99
Create a Custom Patch 107
Delete a Patch 109
Execute Action Menu Options 111
Patch Details Page 112
Patch Information 112
Relationships 115
Devices 116
Patch Requirements 116
Applicability Requirements 116
Patched Requirements 116

A Troubleshooting 117

Patch Management Issues 117
Configuration Issues 124
Error Codes 125

B System Variables 135

Patch Management System Variables 135

About This Guide

This *ZENworks Patch Management Reference* includes information to help you successfully license, configure, navigate, and employ a ZENworks Patch Management system.

Audience

This guide is intended for ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. See ZENworks Documentation.

1 Patch Management Overview

ZENworks Patch Management is a part of the ZENworks product line that provides a fully integrated version of leading patch and patch management solutions for medium and large enterprise networks. Patch Management enables customers to easily translate their organizational security patch policies into automated and continuous protection against more than 90 percent of vulnerabilities that threaten today's enterprise networks. Patch Management ensures that policy measurement and security audits are a true representation of network security status by providing the most accurate and timely vulnerability assessment and patch management available.

- "What's New" on page 9
- "Product Overview" on page 9
- "Supported Environments and Patch Content" on page 10
- "Patch Management Process and Workflow" on page 11

What's New

For more information on What's New in this release, see ZENworks What's New Reference.

Product Overview

Patch Management provides rapid patch remediation, allowing you to proactively manage threats by automating the collection, analysis, and delivery of patches throughout your heterogeneous enterprise to secure end points.

The ZENworks Server has a Web-based management user interface known as ZENworks Control Center. Its Patch Management feature allows you to monitor and maintain patch compliance throughout the entire enterprise. The ZENworks Primary Server can deploy a ZENworks Agent on every client system in the target network, ensuring that all systems are protected with the latest security patches, software updates, and service packs.

The Patch Management feature stays current with the latest patches and fixes by regular communication with external patch source through a secure connection. After the initial 60-day free trial period, the Patch Management feature requires a paid subscription to continue its downloads of the latest patch and vulnerability information.

As part of the ZENworks Agent, a Patch agent is installed on each device that is enabled for Patch Management. The Patch agent analyzes the device to determine what patches it needs, downloads the patches on-demand through the ZENworks content system, and then applies the patches based on the established patching schedule.

To support the ondemand downloading of patches, at least one Ondemand Content Master (OCM) is required. When the OCM receives a device's request for a patch that is not yet available in the ZENworks content system, it downloads the patch from an external site (either the ZENworks patch

repository or a vendor's patch repository), stores it in the ZENworks content system, and serves the patch back to the device. Only Primary Servers can function as OCMs. The Patch Server, when configured, defaults as an OCM. You can add additional OCMs via the Server Hierarchy configuration.

NOTE: ZENworks Patch Management provides software updating and patching services for Windows operating systems and applications, eliminating the need to run the Microsoft Windows Update service. If necessary, however, you can continue to run Windows Update service on the same device as ZENworks Patch Management. Regardless of which solution performs the patch installation, ZENworks Patch Management detects and reports the installation status and source, allowing you to easily monitor the patch compliance of your devices in ZENworks Control Center.

Supported Environments and Patch Content

Platforms that Patch Management supports for installing and operating Patch Management are congruent with system requirements for the ZENworks suite.

Refer to the system components below to see their supported Patch Management platforms:

- Primary Servers
- Satellite Servers
- Managed Devices

For a complete list of requirements for the ZENworks system, see the ZENworks System Requirements.

NOTE: SUSE Linux Enterprise distributions require rpm-python installation as a prerequisite to run the patch scan process. This package is typically installed by default on the ZENworks-supported distributions. If rpm-python is not installed, you must manually install it for the patch scan engine to return an accurate patch status.

Supported patch content: The Patch Management Content Development Team continuously evaluates vendor patch solutions for emerging threats to provide the latest patch content support for operating systems and applications used by ZENworks Patch Management customers.

Due to the evolving nature of patch content support, the ZENworks Patch Management team issues a *Content Quarterly* report with updated information about vendors, products, and product versions that are supported with patch content via the Micro Focus Global Subscription Service (GSS).

To access the latest Content Quarterly, see the report that is relevant to your existing patch feed:

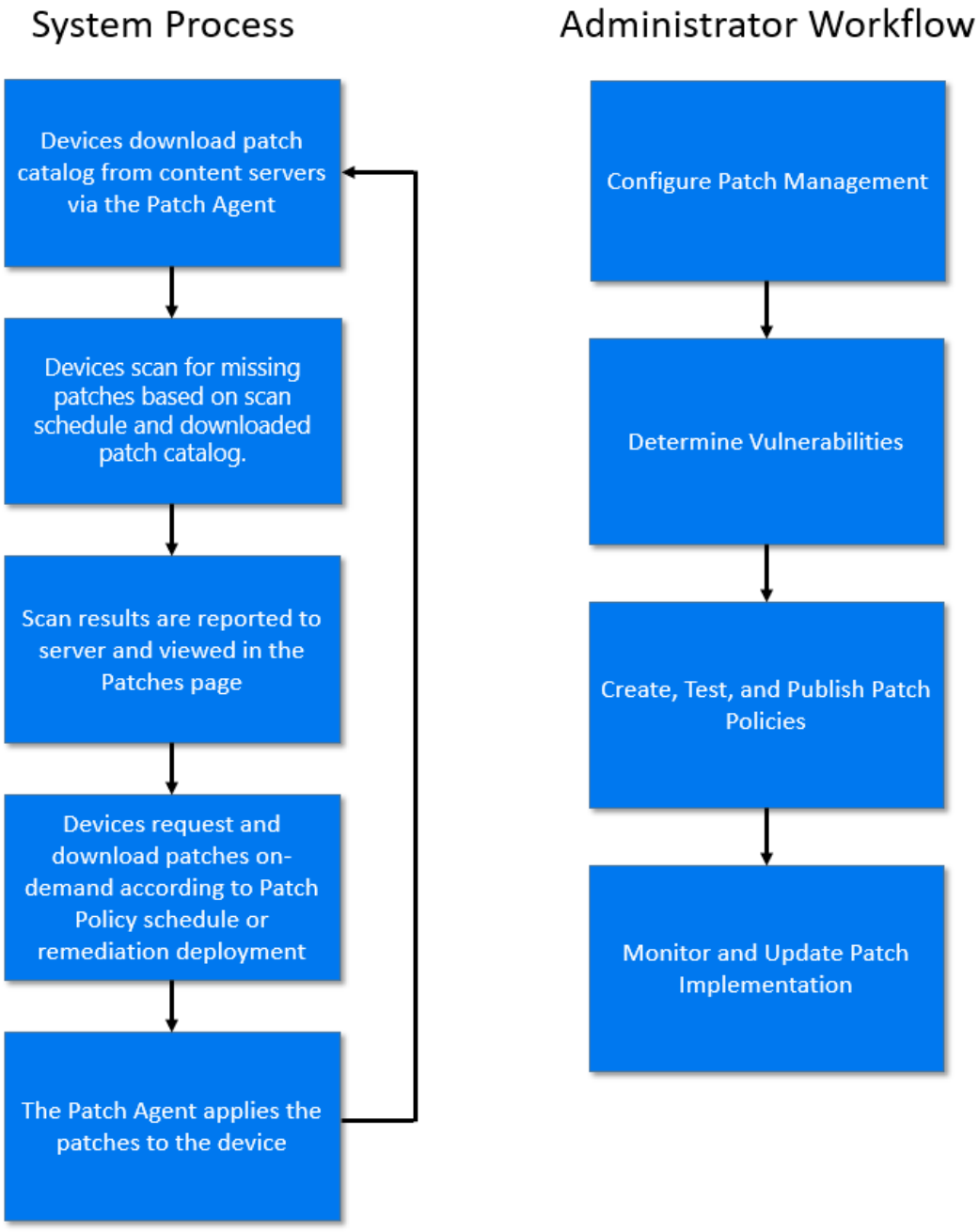
- Patch Content Report - Advanced Patch Feed
- Patch Content Report - Legacy Patch Feed

For relevant ZENworks articles about Microsoft updates, reference the links below:

- ZENworks Patch Management Support for Windows 10 Updates (https://community.microfocus.com/collaboration/zenworks/w/zenworkstips/2240/zenworks-patch-management-support-for-windows-10-updates)
- Patching Microsoft Office 365 (https://community.microfocus.com/collaboration/zenworks/w/zenworkstips/2195/patching-microsoft-office-365)

Patch Management Process and Workflow

The following process maps demonstrate how patch information is communicated between the ZENworks Server and the ZENworks Agent and the general workflow administrators use to implement patch policy across the management zone:



The patch detection cycle begins each day at the ZENworks Server where a Vulnerability Detection task is scheduled for all ZENworks managed devices (servers and workstations).

The ZENworks Agent performs a scan by using the patch catalog on each device, which determines the status (number of Patched or Not Patched devices) for each specific patch.

The results of the patch detection scan are sent to the ZENworks Server and can be viewed anytime in the Security > Patches page. There is also a Patches page for each individual workstation and server.

After completion of the patch detection cycle, devices will either download patches on-demand in accordance with a Patch Policy schedule or when you initiate remediation deployments for applicable devices on the network. If required, you can configure pre-fetch and pre-cache settings to stage and replicate patches to Content servers before they are requested in the ondemand process.

2 Post Migration Tasks

This section explains what native channel patching and software installers are in ZENworks Patch Management and the steps you need to take to enable them in your zone after migrating to the Advanced Patch Platform. It also includes instructions for accessing vendor URLs that require access in your Firewall policies to download patch content via the Patch Service.

- "Enabling Native Update Channel Patching" on page 13
- "Enabling Software Installers" on page 14
- "Enabling Firewall Access to Patch Vendor URLs" on page 15

Enabling Native Update Channel Patching

For most patches, the ZENworks Ondemand Content Masters (OCMs) retrieve the patch content that devices need to install the patches. This includes most Windows and all Mac patches. Some patches, however, are downloaded directly from the vendor source by the native patch mechanism using their native update channel. This includes the following channels:

- SUSE Linux and Red Hat Linux updates
- Windows "Click-to-Run" applications like Microsoft 365 Apps

The patch process is the same for these "native update channel" patches with the exception that the ZENworks content system does not retrieve and distribute the patch content to the device. This means that you can still scan devices for the missing patches, track the patch status in ZENworks Control Center, and schedule and initiate patching via Patch policies or remediation bundles.

However, devices must still be configured to download the patch content from their native update channel.

SUSE and Red Hat Patching

For SUSE and Red Hat patches, you do not need to do any configuration beyond what you have already done to enable Linux patching with the Legacy Patch Platform. For example:

- Register devices you want to patch with SUSE or Red Hat with the respective software update channel.
- Ensure the devices can access the external update channels.

Essentially, if a SUSE or Red Hat device can use its native YaST or YUM package managers to apply updates without ZENworks involved, ZENworks will be able to orchestrate the installation, including tracking the status of patches as well as applying them.

Enable Microsoft 365 Apps Patching

Windows devices use Microsoft's Click-to-Run service to install Microsoft 365 applications like Office 365 and Office 2019. Any Windows device on which you want to apply Microsoft 365 apps must be configured to allow ZENworks to initiate the Click-to-Run service.

To configure a device for Microsoft 365 apps patching:

1. Make sure that the device can apply updates without ZENworks involved.

   For example, make sure that O365 can be updated manually by the user. This ensures that O365 is configured with the correct update channel and the device has access to the update channel.

2. Use Group Policy to enable updates from ZENworks:

   2a Download and install the Administrative Template files (ADMX/ADML) for Office from the Microsoft Download Center.

   2b enable the "Management of Microsoft 365 Apps for enterprise" policy setting.

   You can find this policy setting under Computer Configuration\Policies\Administrative Templates\Microsoft Office 2016 (Machine)\Updates.

3. Alternatively, you can modify the `officeupdate` key in the Windows Registry to add the `officemgmtcom` value set to 1.

Once you complete this configuration on a device, you can track the status of Microsoft 365 Application patches in ZENworks Control Center and initiate the patching just as you would for any other type of patch.

Enabling Software Installers

Software Installers are not really patches at all but are full installations provided for some Windows products. They let you install the product and, in some cases, are required to move from one major version of the product to the next if the normal patch does not provide that upgrade path.

Scanning a device to discover applicable Software Installers significantly increases scan time and significantly increases the number of patch entries in the ZENworks database.

In the Legacy Patch Platform, Software Installers were enabled by default. In fact, there was no way to turn them off. After migration to the Advanced Patch Platform, scanning for applicable Software Installers is turned off so that you can decide if you want to use them.

If you decide to enable Software Installers in the Patch system, you can do it through ZENworks Control Center using a variable. You can enable the variable at the zone, device folder, or individual device level. In general, if you are using Software Installers you will probably want to define the system variable at the zone level so that all Windows devices can scan, install, and report status for Software Installers. But you can set it at a lower level if you wan to target a smaller set of Windows devices.

Enable Software Installers at the Zone Level

To enable Software Installers at the zone level:

1. In ZENworks Control Center, navigate to **Configuration** > **Management Zone Settings** > **Device Management**, and select **System Variables**.
2. Click **Add** in the System Variables panel.
3. Type `scan.software.installers` (all lowercase) in the Name field.
4. Type `true` in the Value field; then click **OK**, and apply the changes.

Enable Software Installers at the Device Folder Level

To enable Software Installers at the device folder level:

1. Select **Devices** in the navigation pane, and click **(Details)** on the device folder where you want to enable Software Installers.
2. Navigate to **Settings** > **Device Management** > **System Variables**.
3. Click **Add** in the System Variables panel.
4. Type `scan.software.installers` (all lowercase) in the Name field.
5. Type `true` in the Value field; then click **OK**, and apply the changes.

Enable Software Installers for an Individual Device

To enable Software Installers for an individual device:

1. Click **Devices** and navigate to, and select, the desired device link in its respective folder.
2. Navigate to **Settings** > **Device Management** > **System Variables**.
3. Click **Add** in the System Variables panel.
4. Type `scan.software.installers` (all lowercase) in the Name field.
5. Type `true` in the Value field; then click **OK**, and apply the changes.

Enabling Firewall Access to Patch Vendor URLs

Once you have migrated Patch Management to the Advanced Patch Platform, you need to ensure that access is configured in your Firewall policies to enable the Patch Service to download patch content for other vendors such as Microsoft and Adobe.

A complete list of vendor URLs is a provided in the spreadsheet below. Download the spreadsheet to access the URLs for your Firewall policies. All ZENworks Primary Servers configured as Ondemand Content Masters must have access.

Download URLs: https://www.microfocus.com/documentation/zenworks-resources/ZPM_URLs.xlsx

3 Configure Patch Management

Before using ZENworks Patch Management, you need to activate the product, start the Patch Service, and configure the Patch Server. All of these settings are designed to be run with left-to-right options in the **Mitigating Vulnerabilities** page of ZENworks Control Center by navigating to Security > Getting Started. More information is provided in the sections below:

- "Activating Patch Management" on page 17
- "Starting the Patch Service" on page 21
- "Configuring the Patch Server" on page 21
- "Configuring the CVE Subscription" on page 23
- "Configuring Patch Pre-Fetch Settings" on page 23
- "Configuring Pre-Cached Content" on page 24
- "Cleaning up Patch Content" on page 25
- "Configuring the Security Dashboard" on page 28
- "Configuring Email Notification" on page 28
- "Configuring the Schedule for Vulnerability Detections" on page 29
- "Initiating a Patch Scan" on page 33
- "Configuring Patch Policy Settings" on page 33
- "Configuring Patch Policy Pre-Install Behavior" on page 37

Activating Patch Management

You can access Patch Management activation settings from the Getting Started page or the Configuration page in ZENworks Control Center:

- **Getting Started page:** Navigate to Security > Getting Started > Mitigating Vulnerabilities, and click the **Activate Product** link in the Enable Patch Management section.
- **Configuration page:** Navigate to Configuration > Licenses panel > Product Licensing, and click the **ZENworks 2020 Patch Management** link.

The Product Activation panel enables management of your product license, as follows:

Evaluate/Activate Product: Either provide a valid product license key, or select **Use Evaluation** to use a temporary license for 60 days. If the evaluation period ends before you provide a valid license key, reference Trial Expired to understand Patch Management behavior after the expiration.

Designate as Production zone: This setting is only applicable if you have a license for Patch Management. You should have already configured this setting as part of the Patch Management migration or installation process by designating your zone as a **production zone** or a **non-production zone** (lab, demo, or test).

Activate the product on all devices in the zone: This option is displayed if the product is in Deactivated state and will be enabled if you select the Evaluate/Activate Product option.

- If you select this option, the product is enabled on all the managed devices in the zone. You can disable the product or the ZENworks agent components at a later time, on selected managed devices at the device folder or the device level.
- If you do not select this option, the product is not enabled across all the managed devices in the zone. You can enable the product or the ZENworks agent components on all devices or on specific devices at a later time, at the zone, device folder, or device level.

Patch Management offers the following licenses:

Table 3-1 *Patch Management Licenses*

License Type	Description
Trial	Denotes trial access to all features of Patch Management for 60 days.
Extended Trial	Denotes continued access to some Patch Management features after the initial 60-day trial, up to 12 months since ZENworks service is installed.
Valid	Denotes a valid product license.
Trial Expired	Denotes that the initial 60-day trial period or the extended trial period has ended, depending on the license in use earlier.
License Expired	Denotes expiry of the current Patch Management license.
Company Name	Name of the company that Patch Management Service is registered to.
Email Address	E-mail address that you can use for receiving alerts and for future communications.
Account ID	Key created by the ZENworks Server, which is passed to the Patch Management Service and used to validate the update request.
Total Non-Expired Licenses	Total number of active licenses. Each registered device requires one license.
Description	The description of the license or the name of the license.
Vendor	The source where the license was purchased.

Depending on the type of license you use, Patch Management functions are enabled as follows:

- **Trial:** All Patch Management capabilities are free to use for 60-days. The 60-day evaluation period starts when you activate the product. If you are upgrading to the latest ZENworks version and are already using the Evaluation mode, the evaluation period will continue for the time remaining until it expires. You can view the expiration date on the main Configuration page > Product Licensing panel or in the Product Activation page.

- **Extended Trial:** On any installation (new or old), you can request a 90-day evaluation key by filling out a form. The 90-day time period starts when the evaluation key is specified. During this license period, only Windows devices have Patch Management support. You can only download new patches released by Microsoft and run Vulnerability Detection for those patches. Patches that were cached previously will have their content cleared so you cannot deploy them. Other features disabled are patch caching, remediation, and generation of reports. In addition, a message appears, asking you to purchase a Patch Management license.
- **Valid:** All Patch Management functions are available.
- **Trial Expired:** After the trial ends, the Server will not download any new patches. All Patch Management functionalities are disabled and you will receive a message asking you to purchase a Patch Management license.

  If ZENworks Configuration Management is not enabled, no new patch signatures or patch content is downloaded. Scanning and remediation using the existing patches will not be stopped, but nothing new will be added.

  If ZENworks Configuration Management is enabled, ZENworks Patch Management continues to download Windows patch signatures so that scans of Windows devices take place and results are reported. However, the patch content cannot be downloaded, so no remediation can occur. This takes place for 1 year.
- **License Expired:** After the license expires, the Server will not download any new patches. However, you can continue to use all Patch Management features on the patches downloaded prior to license expiration.

NOTE: During the evaluation period (keyed or key-less), ZENworks Patch Management is available for all platforms (Windows, Linux, Mac). Devices can be scanned, results reported, and devices patched.

Patch Management provides a 60-day free trial period. You do not need to enter a serial number unless you have purchased the product or the 60-day free trial has expired.

To continue using the Patch Management features of the ZENworks Control Center after your 60-day free trial has ended:

1. Enter a valid serial number for Patch Management.
2. Revalidate the serial number.

The license record is now valid, and displays serial number, status, expiration date, purchased for the License Record.

To validate the serial number and obtain the authorization to download patches, the Primary Server on which patch subscription is being downloaded must have port 443 (HTTPS) access to https://novell.patchlink.com/update, for ZENworks 2017 Update 3 and later, use https://download.novell.com/patchlink for license verification.

The Patch Management content distribution network is a global cache infrastructure with many servers. Downloading patches from this network requires port 80 (HTTP) access to http://novell.cdn.heatsoftware.com/novell/<release_version>.xml. For security reasons, it is also recommended that SSL access to the Internet should be allowed. The **SSL** option is enabled by default and downloads the lists of patches from a secure and trusted site.

You should use nslookup to discover the local IP address for your nearest content distribution node. The content distribution network has over 40,000 cache distribution servers worldwide, plus multiple redundant cache servers in each geographic location. It is important to allow access to a range of addresses through the firewall.

The following table describes each field on the Serial Number page:

Table 3-2 *Patch Management License Items*

Item	Definition
Activate product	Activates the patch management service. The **Patch Management** page is restored in the main panel and the **Patch Management** section is restored in the **Configuration** panel.
Deactivate product	Deactivates the patch management service. The **Patch Management** page is removed from the main panel and the **Patch Management** section is removed from the Configuration page.
Product Serial Number	Patch Management license number (serial number).
Company Name	Name of the company that Patch Service is registered to.
Email Address	E-mail address that you can use for receiving alerts and for future communications.
Account ID	Key created by the ZENworks Server, which is passed to the Patch Service and used to validate the update request.
Total Non-Expired Licenses	Total number of active licenses. Each registered device requires one license.
Description	The description of the license or the name of the license.
Status	Status of license verification. When verification begins, the status reads **Initializing Verification**. When replication ends, the status reads **Completed**.
Vendor	The source where the license was purchased.
Expiration	The date the licenses expire. Typically, licenses expire one calendar year from the date of purchase.
Purchased	The total number of licenses purchased with the product.

After you enter the serial number, you can verify the license by clicking the **Action** drop-down list on the Patch Management License page and selecting **Verify License**.

To start the license verification process, click **Apply**. Automatic verification of the license happens every day with the replication process.

The **Verify License** message box indicates that the verification of the product license is complete or the license has expired.

Starting the Patch Service

The Patch Service runs on each Primary Server and performs functions such as adding new patch metadata and device scan results to the ZENworks database. After it is started, you can monitor its status on the Diagnostics page.

The **Start Patch Service** link becomes active after first activating the product (new install only). You need to click this link, followed by **Start** in the dialog box that opens to start the patch service. As the process runs, a status message is displayed next to the link in the Getting Started page. The status can include any of the following:

- **In Progress**
- **Completed**: The Patch Service is running on all Primary servers.
- **Completed with Issues**: The Patch Service is running on one or more Primary servers.
- **Failed**: The Patch Service failed to start on any Primary servers.

In the event that you get a status of **Completed with Issues** or **Failed**, the status text will become a link that you can click to be prompted for further actions to take to fix the issue.

Configuring the Patch Server

The Patch Server Configuration settings define the server for patch-related maintenance tasks as well as the default server for an Ondemand Content Master. To access these settings, navigate to Security > Getting Started > Mitigating Vulnerabilities, and click **Select Patch Server** in the Enable Patch Management section. You can also access the settings under Security in the Management Zone Settings.

Patch Server

One Primary Server needs to be designated as the Patch Server to perform Patch-related maintenance tasks for your zone. This server also functions as an Ondemand Content Master (OCM) by default. The OCM fetches patches from the ZENworks and vendor patch repositories when they are needed by devices. If you designate one or more additional Primary servers as OCMs in the zone, the OCM designation can be removed from the server selected in this configuration as the Patch Server. You can make that change via the Server Hierarchy configuration.

Any Primary servers designated as OCMs need to meet the Ondemand Content Master requirements. For more information, see

Maintenance Schedule

The Patch Server performs maintenance once a day, which includes rebuilding the patch scan files (DAU bundles), disabling outdated patches, and generating an email notification.

You can define the time that scheduled maintenance occurs and run a manual maintenance task at will.

Reset ZENworks Patch Management

This option enables you to set all Patch Management settings, including deployments and patch policies, back to the default state. All patch-related configuration settings, policies, deployments, and data will be removed from the database. The patch content stored on the Content Server will be cleaned up based on the Ondemand Content clean-up schedule for each server.

When you initiate the Patch Management Reset, the following actions will be performed:

- Patch Management Settings clean-up
- Database clean-up
- Patch Bundle clean-up
- Patch Policy clean-up
- Patch Settings clean-up
- If the Patch license is currently in the evaluation mode or all licenses have expired, then the evaluation period will be reset so that you can evaluate ZPM again. The current valid licenses will remain unchanged.
- Patch services will be stopped on all the servers.

Before resetting the Patch Management:

- Ensure that the CVE subscription, Bundle or Device deletion is not in progress.
- Ensure that the Patch Maintenance is not in progress.

Ondemand Content Master - Requirements

The Ondemand Content Master requires an Internet connection to communicate with and download content from external sites.

Configuring a proxy: If the OCM requires a proxy to access the service, the OCM server's Subscription proxy configuration file is used.

If you have configured your network to use a proxy server, you must configure the proxy server subscriptions.

1. On the Primary Server on which the Ondemant Content Master is configured to run, navigate to the `lpm-server.properties` file.
   - Linux: `/etc/opt/microfocus/zenworks/`

   An example of the content within the `lpm-server.properties` file is displayed below:

   ```
   Debug=false
   TTL=24
   subscription-proxyaddress=
   subscription-proxyport=
   subscription-proxyuser=
   subscription-proxypassword=
   subscription-useNTLM=false
   ```

2 Modify and save the file with the following subscription proxy details:

- Set the value of `subscription-proxyaddress` to the IP address of the proxy server.
- Set the value of `subscription-proxyport` to the port number of the proxy server.
- (Conditional) If the proxy is authentication-based, set the value of `subscriptionproxyuser` to the name of the proxy user.
- (Conditional) If the proxy is authentication-based, set the value of `subscriptionproxypassword` to the password associated with the proxy user name.
- It is recommended to use the `zman srpp` command to specify an obfuscated password instead of specifying the raw password.
- (Conditional) If the proxy server uses an NTLM realm, set the value of `subscriptionuseNTLM` to true. By default, the value is false.

3 Restart the ZENworks services.

Accessing the CDN: The following URL must be open to access the CDN: `https://microfocus-2dcb60a8-26c9-4560-9cc2-34a16ea5f6e6.2d7dd.cdn.bitdefender.net`

Configuring the CVE Subscription

With Patch Management you can view the patches that are published and identify if the devices in your zone are vulnerable or not. However, information about the vulnerabilities being addressed by the patch is not easily available. You have to either know the CVE Identifier or you have to check the patch details to identify the vulnerability being addressed by the patch. ZENworks provides an enhanced security view into the vulnerabilities on the devices by providing the capability to map Common Vulnerabilities and Exposures (CVE) to the related patches in ZENworks. To use this capability you need to configure the CVE subscription.

You can access the **Subscriptions** page where you need to configure the CVE Subscription via one of the navigation options below:

- **Subscribe and Share** in the navigation panel
- **Mitigating Vulnerabilities** page when navigating to Security > Getting Started

For specific information about configuring the CVE Subscription, see Mitigating Vulnerabilities Using CVEs in the ZENworks - CVE Reference.

Configuring Patch Pre-Fetch Settings

Beginning in ZENworks 2020 Update 3, Patch Management enhancements incorporate ondemand patching of devices. In principle, this means that patches required by managed devices are not downloaded to Content servers until they are requested by the device. However, there are options that you can configure to pre-fetch patch content from external sources before the patches are requested by devices. You can also configure pre-cache settings to replicate patches to specified Content servers once they are downloaded by an Ondemand Content Master. These settings are described in Configuring Pre-Cached Content.

Pre-fetch settings are described below. To access the settings in ZENworks Control Center, navigate to Configuration > Management Zone Settings > Security > Patch Pre-Fetch Settings.

For additional information about pre-fetching content, see Understanding Pre-Fetching and Pre-Caching of Patches.

Pre-Fetch Actions

Each pre-fetch option is described below:

- **Manual "Update Cache" action**: This option is selected by default. When enabled, a patch is not downloaded by an Ondemand Content Master until the first device that needs it requests it or you select the patch in the Patches page and run **Update Cache** from the action menu.
- **Patch policy rebuild**: When enabled, this option will pre-fetch patches required by devices that meet the patch policy criteria upon policy rebuild.
- **Patch remediation deployment**: When enabled, this option will pre-fetch patch content applicable to remediation deployments, so the content is already fetched when requested by devices.

Languages

With ondemand patching, the required patch language is included with the patch request from the managed device. However, if you pre-fetch patches before a device requests them, the language must be specified. Use the Languages panel to select the patch language or languages required when enabling any of the pre-fetch actions.

Configuring Pre-Cached Content

Pre-caching replicates content that is already found on a Content Server, which can include content already requested by a device, content that is pre-fetched based on Pre-Fetched Settings, or both.

You can configure pre-caching of content for specified Primary servers and Satellites in the zone. If required, you can also override the zone settings on individual servers or Satellites. Satellites designated for pre-caching at the zone level or individually must already be configured for a Content role. For information, see Adding and Configuring Satellite Devices in the *ZENworks Primary Server and Satellite Reference*.

Pre-cached content settings are described below. To access the settings in ZENworks Control Center, navigate to Configuration > Management Zone Settings > Bundle, Policy and Content > Pre-Cached Content.

For additional information about pre-caching content, see Understanding Pre-Fetching and Pre-Caching of Patches.

Content Types

See the descriptions below to understand the pre-cached behavior for each content type. When selected, the content type is pre-cached to servers specified in the Content Servers panel.

Pre-cache content for:

- **Bundles:** Pre-caches content associated with bundles to the Primary Servers and Satellites included in the Content Server list.

- **Policies:** Pre-caches content associated with policies to the Primary Servers and Satellites included in the Content Server list.
- **System Updates (Satellites only):** Pre-caches System Updates to the Satellites specified in the Content Servers list.

  NOTE: Because Primary Servers require that System Updates be cached locally, System Updates are always pre-cached to all Primary Servers regardless of whether they are included in the Content Servers list.

Additional content types included with a new installation or after migrating Patch Management:

- **Windows Patches:** Pre-caches Windows patches that are fetched for remediation deployments or patch policy distribution
- **Mac Patches:** Pre-caches Mac patches that are fetched for remediation deployments or patch policy distribution
- **Linux Patches:** Pre-caches Linux patches that are fetched for remediation deployments or patch policy distribution

Content Servers

All Primary servers are Content servers, so you can add any Primary Server in the zone for pre-caching content that you specify in the Content Types panel. You can also add any Satellite that is configured with a Content role.

Use the **Add** option to specify Content servers (Primary servers and Satellites) for pre-caching content.

If required you can also enable the options to automatically pre-cache content for new Primary Servers and Satellites added to the zone at a later time.

Overriding Zone Pre-Cached Settings

If you want to override the zone pre-cached settings for a specific Primary Server or Satellite in the Content Servers list, do the following:

1. Navigate to **Devices** > **Servers** (or **Workstations**) and click the Primary Server or Satellite link.
2. Select **Settings** > **Security** > **Pre-Cached Content**.
3. Click the **Override** link to enable the configuration.
4. Modify the existing settings and **Apply** the changes.

Cleaning up Patch Content

Using the CVE and Patch Cleanup page, you can delete disabled patch content and data, as well as delay the disabling of superseded patches and patches that are no longer required by ZENworks.

To configure patch cleanup settings, click **Configuration** in the ZENworks navigation menu, and go to **Configuration** > **Security** > **CVE and Patch Cleanup**.

Refer to the descriptions below to understand and configure the cleanup settings according to your organization's needs:

Item	Description
CVE Cleanup	The CVE Cleanup setting is applicable to both, the CVE data and the CVE trend data. Using this setting you can specify the number of years after which the CVE data (unmodified CVEs) and the historical trend data stored for the CVEs are deleted from ZENworks. By default, the value is configured as 5 years. Therefore, CVEs that have not been modified for 5 years, along with the historical CVE trend data of 5 years are deleted from ZENworks. The CVE Cleanup will be performed during the next subscription run. To delete the CVE data and the CVE trend data sooner or later than the default 5 years, you can specify the required value in the **Delete CVEs after x years** field. **NOTE:** The CVE trend data is stored for a maximum of 10 years and it is calculated from the time when Vertica was configured in the zone. Therefore, if you specify the CVE Cleanup as a value above 10, for example, 14 years, the unmodified CVEs will be deleted after 14 years, but the historical trend data will be deleted after 10 years.
Disabled Patch Cleanup	Specify the time period after which to delete data for a disabled patch. This setting deletes the patch listing for a patch that meets the following conditions: ◆ The patch is disabled. ◆ The patch has been disabled longer than the time duration selected from the drop-down. **Delete disabled patch data after:** Specify when the disabled patch data should be deleted from ZENworks. The default value is 5 years.

Item	Description
Superseded Patches Disablement	By default, when a patch is superseded by a newer patch, it is disabled and can no longer be applied to devices. In general, this is the desired behavior because best practice dictates that you keep devices updated with the most recent patches in order to minimize security risks. However, you might have situations where you need a superseded patch to remain enabled. The following settings let you change when superseded patches become disabled: ◆ **Delay the disabling of superseded patches for:** Specify for how long you want to delay the disabling of superseded patches. Based on your requirements, you can specify the delay days between 1 and 180. However, this setting is NOT recommended as postponing patch updates that are superseded increases the risk to your environment. **NOTE:** You can also configure the PATCH_DELAY_SUPERSEDED_DISABLE system variable which overrides the Delay the disabling of superseded patches for settings. For more information about this system variable, see "PATCH_DELAY_SUPERSEDED_DISABLE" on page 136 ◆ **Do not disable superseded patches that are included in a policy:** By default, a superseded patch is not removed from a policy and replaced by the superseding patch until the policy is rebuilt and republished. This behavior can result in a period of time where the policy does not apply the superseded patch (because it is disabled) or the new superseding patch (because it is not in the policy). You can use this setting to ensure that patches that are included in a policy are never disabled as long as they are in the policy. Patches that are included in the policy via a rule remain enabled until they are removed when the policy is rebuilt. Patches that are included via the Members list remain enabled until they are manually removed from the list and the policy is rebuilt. Also, if a user enables a superseded patch that is within a policy, but there are no applicable devices, then, on the next service update, the patch will get disabled, even though this option is selected. **IMPORTANT:** The "Do not disable superseded patches that are included in a policy" option is deprecated. Hence, this option will be hidden after migrating to the Advanced Patch Feed.

Item	Description
Superseded Patches Disablement (Cont.)	**NOTE:** ◆Both settings apply only to patches that are superseded after the setting is enabled. ◆ In the Advanced Patch Feed, the above settings cause superseded patches to remain enabled in the ZCC UI; this allows you to see the Patched/ Not Patched status of devices. However, the superseded patches will not be installed on devices. For example, if you have enabled the **Do not disable superseded patches that are included in a policy** when a patch in the policy is superseded, it will remain enabled in the ZCC UI, but it will not be installed (if needed) on a device. Or, if you enable the **Delay the disabling of superseded patches for** option and then try to install a superseded patch via a Remediation Deployment, it will not install.
Patches Disablement	These settings disable patch data in the system based on the criteria you select. Both options are selected by default. ◆ *Detect only the current supported Service Packs* This setting enhances the timeliness of deploying the latest service pack patches to managed devices, as opposed to scanning for non-applicable patches. ◆ *Disable older patches by age* This setting enables you to delete patches based on when they were released by the OS Vendor or a Third-party Vendor.

Configuring the Security Dashboard

For information about the Patch Management Dashboard, see Employing the Security and Patch Dashboard.

Configuring Email Notification

Use the Email Notifications page to define the users who receive emails notifications whenever new patches are detected or Patch policies are rebuilt. The email notification is generated by the Patch Server during its scheduled maintenance period.

In addition to the procedure below, using Email Notification requires the following:

- Configuring an SMTP Server
- Configuring the Primary Server that will connect to the SMTP Server.

To configure the Primary Server, go to Configuration > Event and Messaging > Notification Servers. Click the browse icon and then select a Primary Server that sends patch management related E-mail notifications. This is an optional field. If the server is not configured, then by default, notifications will be sent from the server on which patch server is running.

IMPORTANT: ◆This is a new requirement beginning in ZENworks 2020 Update 3 (new installations or upgrades that have migrated Patch Management from earlier 2020 versions).

- If you are facing any issues, then see system messages. In ZCC, go to Audit and Messages > System Messages.

To configure Email Notification:

1. Select **Configuration** in the ZENworks navigation menu, and go to **Configuration** > **Security** > **Email Notification**.
2. In the **Patch Email Notification** field, type the desired email addresses in the **From**, **To**, and **CC** fields.
3. Click **Apply** to save changes.
4. Click the **Notification Servers** link in the Email Notification panel to go to that configuration and configure the SMTP Server and the Primary Server connection to it.

   More information about the Notification Servers configuration is found in the Help on that page.

Configuring the Schedule for Vulnerability Detections

The Vulnerability Detection Schedule page enables you to configure Vulnerability Detection schedules for the devices in your network. You can decide when to run the Vulnerability Detection on network devices as well as specify when to distribute bundle content through Vulnerability Detection.

To configure the Vulnerability Detection Schedule, select **Configuration** in the ZENworks navigation menu, and go to **Configuration** > **Security** > **Vulnerability Detection Schedule**.

NOTE: If you want to make changes to the schedule of a DAU Bundle, you should configure it within the Vulnerability Detection Schedule page. If the DAU bundle schedule is modified within any other page of ZCC, such as the Device's Assignments or the Bundle's Relationship page, under Assignment Details, it will be overridden during the next service update by the value configured in the Vulnerability Detection Schedule page.

Refer to the descriptions below to understand which configuration options to choose for running Vulnerability Detection:

Item	Description
Distribute vulnerability definition before scan	Lets you deploy bundle content immediately.
Distribute vulnerability definition content on a schedule	Lets you specify a schedule when Vulnerability Detection bundles will be distributed to devices.

Item	Description
Check for vulnerabilities on device refresh	Lets you initiate Vulnerability Detection action when the Agents on the managed devices are refreshed.
Check for vulnerabilities on a schedule	Lets you specify a schedule when the Vulnerability Detection will run.

Patch Management offers two types of schedules to determine when a Vulnerability Detection is run and bundle content is distributed, Date Specific and Recurring.

- **Date Specific:** Select Date Specific to schedule the deployment to your selected devices according to the selected date.

  Set the following options in the Date Specific page:

  - ***Start Date:*** Enables you to pick the date when you need to start the desired action. To do so, click the Plus icon to open the calendar and pick the date. To remove the selected date, click the Minus icon.
  - ***Run event every year:*** Ensures that the desired action starts on a selected date at a selected time, repeats every year, and if defined, ends on a specific date.
  - ***Process immediately if device unable to execute on schedule:*** Ensures that the desired action starts immediately if the device could not execute on the selected schedule.
  - ***Select when schedule execution should start:*** There are two options that enable you to select the start time of the schedule execution namely:
    - Start immediately at Start Time: Deactivates the End Time panel and starts the action at the start time specified. In this option, you must set the start time in the Start Time panel:

    - Start at a random time between Start Time and End Times: Activates the End Time panel next to the Start Time panel. You can specify the end time and the start time so that the action occurs at a random time between them. The End Time panel appears as follows:

    In both time panels, the first drop-down list enables you to select the hour, the second drop-down list enables you to select the minute, and the third drop-down list enables you to select am and pm.

    Selecting the Use Coordinated Universal Time check box enables you to schedule the desired action at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at the local time.

- **Recurring:** Select Recurring to start the deployment on the selected day at a selected time, repeat the deployment every day/week/month, and if defined, end on a specific date.

Set the following options in the Recurring page:

- ***When a Device is Refreshed:*** This option enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

  To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time to delay the deployment:

  NOTE: The device is refreshed based on the settings in **Configuration** > **Device Management** menu > **Device Refresh and Removal Schedule** (Manual Refresh or Timed Refresh). Alternatively, you can refresh the device by selecting a device in the **Devices** page and clicking the **Refresh Device** option in the **Quick Tasks** menu.

- ***Days of the Week:*** This option enables you to schedule the deployment on selected days of the week.

  To set the day of deployment, select the **Days of the week** button, select the required day of the week, and set the start time of deployment.

  If you click the **More Options** link, additional deployment options appear:

  - Selecting the **Use Coordinated Universal Time** check box enables you to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.
  - Selecting the **Start at a random time between Start Time and End Times** check box activates the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between the start and end times.
  - The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and, if defined, end at the specific time. This option also enables you to restrict the deployment to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box, and click the **Calendar** icon to open the calendar and pick a start date or end date.

- ***Monthly:*** This option enables you to specify the monthly deployment options.

  In the Monthly deployment option, you can specify the following:

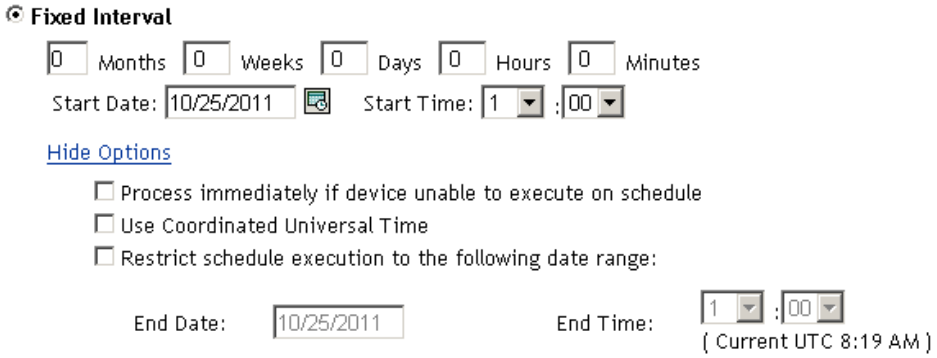
  - **Days of the month:** Enables you to schedule the deployment on a specific day of the month. You can specify any number between 1 and 31.
  - **Last day of the month:** Enables you to schedule the deployment on the last day of the month.
  - **Particular days of the month:** Enables you to schedule the deployment on specific days of every month. The valid options for the day are first, second, third, fourth, and fifth. The valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows.

To select an additional day of the month, click the **Plus** icon and use the drop-down arrows in the second row. To remove a particular day from the list, click the **Minus** icon.

If you click the **More Options** link, additional deployment options appear.

NOTE: The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and, if defined, end on the specific time. This option also enables you to restrict the deployment to the period between the **Start Date** and the **End Date**. To set this option, select the **Restrict schedule execution to the following date range** check box, and click the **Calendar** icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

- ***Fixed Interval:*** This option enables you to schedule a recurring deployment that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule, as shown in the following figure:



If you click the **More Options** link, additional deployment options appear.

Setting Vulnerability Detection at the Folder Level

The Vulnerability Detection schedule can also be set at the folder level which enables you to set the deployment options for Vulnerability Detection for the Server or Workstation estate. By configuring Patch Management settings at the folder lever you will override the System settings (configured in the Configuration page), however, you can return to the System settings at any time by using the Revert option.

To configure the Vulnerability Detection Schedule at the folder level:

1. Click **Devices** in the ZENworks navigation menu.
2. Click the **Details** link on the folder you would like to configure settings for.
3. Go to **Settings** > **Security** > **Vulnerability Detection Schedule**.
4. At the top of the page there is an option to **Override the System** settings, select this to begin making changes.

NOTE: This option can be used to revert back to System settings if you need to change back.

5 Select your desired schedule for the Vulnerability Detection, as described in Configuring the Schedule for Vulnerability Detections.

Initiating a Patch Scan

Use this quick task to update the Primary Server with required patches for one or more selected devices without waiting for a scheduled scan so that patches can be identified for installation, and any pre-fetching or pre-caching that may apply. The actions and results for the different Patch Scan options are explained in more detail below:

NOTE: To initiate the patch scan, it is recommended that at least 500 MB of free disk space is available.

ZENworks Patch Management will not be detected on Appliance and OES devices.

Scan using updated patch scan signature (DAU) file

This default option retrieves the latest information from the patch catalog to scan selected devices. If there are patches required for the selected devices that are not in the Patches list, the scan will upload that information to the server.

Scan using device's current patch scan signature (DAU) file

This option scans the selected devices using the patch catalog currently available on each device and uploads the results of required patches to the server. The uploaded results might not be from the latest catalog for applicable devices.

No scan; retrieve existing scan results only

This option uploads or refreshes the results of the last patch scan that occurred for each selected device. The uploaded results might not include all patches from the current patch catalog on each device and/or the latest patch catalog available.

Configuring Patch Policy Settings

Patch Policy Settings are used to define enforcement times and reboot behaviors for each patch policy.

NOTE: If you want to make changes to the schedule of a Patch Policy, you should configure it within the Patch Policy Settings page. If the schedule is configured within any other page of ZCC, such as Device's Assignments or the Bundle's Relationship page, under Assignment Details, it will not override the schedule that was previously defined in the Patch Policy Settings page. Instead, it will be run multiple times, based on the schedule configured within each page.

- Schedule Enforcement: When configuring **Schedule Enforcement**, you can leave the default setting to manually apply patches on the agent device using the “zac pap” command in the Command Line Utility (zac), or you can define a schedule when patches will automatically be applied.
- Patch Policy Reboot Behavior: When configuring **Patch Policy Reboot Behavior**, you can leave the system defaults in place (no reboots or prompts), or you can define how users are prompted and interact with device reboots when patches are applied.

Schedule Enforcement

You can schedule dates and times that your Patch Policies are pushed out. This feature is useful for distributing and enforcing Patch Policies during off hours, thus decreasing network traffic and strain. The idea is that a policy can be scheduled to be released at different times or outside of working hours. Using this configuration will affect all policies that are set up and will set the schedule for the deployment.

NOTE: Before you can schedule Patch Policy enforcement, a patch policy must be created. Click **Security** in the navigation menu, and select the **Patch Policies** page. Make sure a patch policy exists. If you have to create a new one, make sure the system has time to download the patches.

- **Default (Manually apply patches on the agent using “zac pap”):** This configuration is the system default and requires manually implementing patch policies using the zac Command Line Utility.
- **Schedule patch policy application time:** This configuration enables setting a schedule to automatically apply patches, which includes the option to limit the duration time of patch installation based on a specific date or a recurring schedule.
  - ***Restrict Duration:*** If you check the **Restrict Duration** check box, you can limit how long patches are applied by entering a time increment based on the number of hours, minutes, or a combination of both.
  - ***Date Specific:*** If you choose the **Date Specific** schedule type, you can schedule patch deployment using the following criteria:
    - **Start Date(s):** Enables you to pick the date when you need to start the deployment.
    - **Run event every year:** Ensures that the deployment starts on a selected date at selected time and repeats every year. If defined, ends on a specific date.
    - **Process immediately if device unable to execute on schedule:** Ensures that the deployment starts immediately if the device was unable to execute on the selected schedule.

- **Select When Schedule Execution Should Start:** There are two options to enable you to select the start time of the schedule execution namely:
  - **Start Immediately at Start Time:** Deactivates the **End Time** panel and starts the deployment at the start time specified. In this option, you must set the start time in the **Start Time** panel.
  - **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between them.

    NOTE: Selecting the **Use Coordinated Universal Time** check box enables you to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.

- ***Recurring:*** If you choose the **Recurring** schedule type, you can schedule patch deployment using the following criteria:
  - **When a device is refreshed:** Enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

    To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time by which you require delaying the deployment.

    By default, the patch bundle install frequency is set to Install once per device. For a recurring deployment, change it to Install always.

    1. Click the **Actions** page for the particular patch bundle assignment.
    2. Click **Options**. This opens the Install Options window.
    3. Select **Install always** and click **OK**.
    4. Click **Apply**.

    NOTE: The device is refreshed based on the settings in **Configuration** > **Device Management** menu > **Device Refresh and Removal Schedule** (Manual Refresh or Timed Refresh). Alternatively, you can refresh the device by selecting a device in the **Devices** page and clicking the **Refresh Device** option in the **Quick Tasks** menu.

  - **Days of the week:** Enables you to schedule the deployment on selected days of the week. To set the day of deployment, select **Days of the week**, select the day of the week, and set the start time for the deployment.
  - **Monthly:** You can schedule the deployment on a specific day of the month, the last day of the month, or a specific day every week or month.
  - **Fixed Interval:** Enables you to schedule a recurring deployment that runs on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule.

Patch Policy Reboot Behavior

Some patches require their host to be rebooted after installation. You can leave the default of no reboots or prompts and handle these actions another way, or you can choose to notify users when a reboot is required and also give them some flexibility for when the reboot takes place.

Refer to the reboot options described below to better understand how to configure them:

- **Default Disabled (no reboots or prompts):** The default option is typically used when zone administrators have other processes in place that handle reboots on a routine basis.
- **Enabled:** Select this option to allow reboots when patching and to enable the Notify Users check box.
- **Notify Users:** Select the check box to enable reboot notification and its configuration options.
  - ***Description text:*** Edit the text of the notification prompt when Notify Users is selected.
  - ***Options:*** Define how the user is notified of and interacts with the reboot. There are three options:
    - **Suppress reboot:** Select **Yes** to prevent the reboot.

      NOTE: Selecting **Yes** also prevents the notification prompt. However, the following system variable can be used to enable the prompt while still repressing the reboot:

      `PATCH_ALWAYS_SHOW_REBOOT_PROMPT`

      For more information about this variable and setting system variables in general, see Patch Management System Variables.

    - **Allow User to cancel:** Select **Yes** to enable a cancel option in the reboot notification prompt.
    - **Allow User to snooze:** Select **Yes** to enable a snooze option in the patch policy reboot notification prompt, which delays the reboot.
      - **Snooze interval:** The duration the reboot is delayed when the user clicks Snooze.
      - **Reboot within:** The deadline when the user can no longer delay the reboot.
      - **Show tray notification:** If you select this option, a notification for a pending reboot is displayed in the system tray. Notification options include the following:
        - *Tray notification duration:* Enter a value in hours, minutes or seconds for how long the system tray notification is displayed before being hidden.
        - *Tray notification text:* Edit the text you want to appear in the notification prompt.

IMPORTANT: ◆If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

- If you enable Notify Users and force a reboot (Suppress Reboot = No), the reboot will occur after the Reboot within the interval has expired (2 hours by default), regardless of the other settings (Allow user to cancel, Allow user to snooze, and Snooze interval). If you want the

reboot to occur sooner, you can set the Reboot within the interval to a shorter time such as 10 minutes. If you want the reboot to occur immediately, set it to 0 hours, although this is not recommended as it will not give users time to save their work.

Configure Patch Policy Settings at the Folder Level

Patch Policy Settings can also be set at the folder level which enables you to set patch enforcement and reboot behavior for the Server or Workstation estate. By configuring Patch Management settings at the folder lever you will override the System settings (configured in the Configuration page), however, you can return to the System settings at any time by using the Revert option.

To configure the Patch Policy Settings at the folder level:

1. Click **Devices** in the ZENworks navigation menu.
2. Click the **Details** link on the folder you would like to configure settings for.
3. Go to **Settings** > **Security** > **Patch Policy Settings**.
4. At the top of the page there is an option to **Override** the system settings, select this to begin making changes.

   NOTE: This option can be used to revert back to System settings if you need to change back.

5. Configure Schedule Enforcement and Patch Policy Reboot Behavior sections for the folder.

Configuring Patch Policy Pre-Install Behavior

In Patch Policy Pre-Install Behavior you define when patches are distributed to the agents and how end users are notified of the patch installations.

- Schedule Distribution: When configuring **Schedule Distribution**, you can leave the default setting, which distributes patches according to the configuration in Patch Policy Settings, or you can define a schedule for patch distribution.
- Pre-Install Notification Options: When configuring **Pre-Install Notification Options**, you can leave the system defaults in place, or you can override the system settings and define how end point users are prompted and interact with patch installations.

Schedule Distribution

The Schedule Distribution page allows you to define whether users receive notification when patches are downloaded and installed, and to customize the installation settings.

- **Default (Distribution and enforcement will apply on enforcement schedule):** Use this option to stay with the **Schedule Enforcement** settings defined in **Patch Policy Settings.**
- **On Device Shutdown:** Use this option to deploy patches on device during shutdown or reboot.

- **Schedule patch policy application time:** Select this option to override the default options and choose new ones. This option enables setting a schedule that can limit the duration time of patch installation based on a specific date or a recurring schedule.
  - ***Restrict Duration:*** If you check the **Restrict Duration** check box, you can limit how long patches are applied by entering a time increment based on the number of hours, minutes, or a combination of both.
  - ***Date Specific:*** If you choose the **Date Specific** schedule type, you can schedule patch deployment using the following criteria:
    - **Start Date(s):** Enables you to pick the date when you need to start the deployment.
    - **Run event every year:** Ensures that the deployment starts on a selected date at selected time and repeats every year. If defined, ends on a specific date.
    - **Process immediately if device unable to execute on schedule:** Ensures that the deployment starts immediately if the device was unable to execute on the selected schedule.
    - **Select When Schedule Execution Should Start:** There are two options to enable you to select the start time of the schedule execution, namely:
      - **Start Immediately at Start Time:** Deactivates the **End Time** panel and starts the deployment at the start time specified. In this option, you must set the start time in the **Start Time** panel.
      - **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between them.

      NOTE: Selecting the **Use Coordinated Universal Time** check box enables you to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.

  - ***Recurring:*** If you choose the **Recurring** schedule type, you can schedule patch deployment using the following criteria:
    - **When a device is refreshed:** Enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

      To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time by which you require delaying the deployment.

      By default, the patch bundle install frequency is set to **Install once per device.** For a recurring deployment, change it to **Install always**, after completing the patch policy. For more information, see "Install Action Set Options" in the *ZENworks Software Distribution Reference*.

      NOTE: The device is refreshed based on the settings in **Configuration** > **Device Management** menu > **Device Refresh and Removal Schedule** (*Manual Refresh* or *Timed Refresh*). Alternatively, you can refresh the device by selecting a device in the **Devices** page and clicking the **Refresh Device** option in the **Quick Tasks** menu.

- **Days of the week:** Enables you to schedule the deployment on selected days of the week. To set the day of deployment, select **Days of the week**, select the day of the week, and set the start time for the deployment.
- **Monthly:** You can schedule the deployment on a specific day of the month, the last day of the month, or a specific day every week or month.
- **Fixed Interval:** Enables you to schedule a recurring deployment that runs on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule.

To save any changes made in **Patch Policy Pre-Install Behavior** options, click **Apply**.

Pre-Install Notification Options

The Pre Install Notification Options page allows you to define whether users receive notification when patches are downloaded and installed, and to customize the installation settings.

- **Use values assigned to system variables or defaults:** Select this option to use the default pre-install notification options defined within the Pre-Install Notification settings.
- **Override Settings:** Select this option to override the default options and choose new ones. Selecting this option makes the remaining options available.
  - ***Notify Users of Patch Install:*** Select this option to notify the user prior to the installation of the patch.
  - ***Description text:*** The text of the notification message. You can edit this field only if you override the default settings.
  - ***Options:*** When you define installation options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or the custom settings. There are three options:
    - **Allow User to cancel:** Allows the user to cancel the patch installation.
    - **Allow User to snooze:** Allows the user to delay the installation.
      - **Snooze interval:** The duration the install is delayed when the user snoozes.
      - **Install within:** The deadline that the user can no longer snooze the installation.

      NOTE: Even if you snooze the installation, the popup window will continue to appear every few seconds until you proceed with or cancel the installation.
    - **Show tray notification:** On selecting this option, a notification for a pending installation is displayed in the system tray. If you select this option, define the following:
      - **Tray notification duration:** Enter a value in hours, minutes or seconds for how long the system tray notification is displayed before being hidden.
      - **Tray notification text:** Type the text you want to appear in the notification.

To save any changes made in **Patch Policy Pre-Install Behavior** options, click **Apply**.

Configure Patch Policy Pre-Install Behavior at the Folder Level

Patch Policy Pre-Install Behavior can also be set at the folder level, which enables you schedule patch distribution and set pre-install notification options for the Server or Workstation estate. By configuring Patch Management settings at the folder lever you will override the System settings (configured in the Configuration page), however, you can return to the System settings at any time by using the Revert option.

To configure the Patch Policy Pre-Install Behavior at the folder level:

1. Click **Devices** in the ZENworks navigation menu.
2. Click the **Details** link on the folder you would like to configure settings for.
3. Go to **Settings** > **Security** > **Patch Policy Pre-Install Behavior**.
4. At the top of the page there is an option to **Override** the system settings, select this to begin making changes.

   NOTE: This option can be used to revert back to System settings if you need to change back.

5. Configure Schedule Distribution and Pre-Install Notification Options sections for the folder.

4 Assess Vulnerabilities

After configuring vulnerability detection, licensing, and other settings, you can assess device vulnerabilities via the Security pages, Device patches, and the ZENworks Reporting console. You can also take steps to manage patch compliance from the Dashboard, Patch Policies, and Patches pages.

- "Security Pages" on page 41
- "Viewing Patches for a Device" on page 50
- "Accessing Patch Management Reports" on page 53

Security Pages

The Security pages are where the majority of patch-related activities are performed, to include monitoring all patches across all systems registered to the ZENworks Server. From here you can assess patch compliance, view recently released patches, check the last time each device was scanned for patch compliance, search for patches, create custom patches, create and manage patch policies, and more.

- "Employing the Security and Patch Dashboard" on page 41
- "Viewing Patch Policies" on page 48
- "Viewing Zone Patches" on page 48
- "Viewing Patch Status" on page 49

Employing the Security and Patch Dashboard

The Patch Dashboard has three default dashlets that provide a comprehensive snapshot of key indicators, so you can quickly assess the overall health and compliance of patches on devices in your zone. You can also initiate action directly from respective dashlets, when expanded, to remediate, download, or disable selected patches, to discover patches, to reconfigure the zone vulnerability detection schedule, and to view patch and device details.

The Security Dashboard has four dashlets that enable you to quickly assess the vulnerability status of your zone. Using these dashlets you can track patches and CVEs, identify the top CVEs in the zone and the CVE severity distribution details. Using these dashlets you can deploy remediations, and perform patch scans.

Custom dashlets: You can create custom dashlets from any of the default dashlets or from other custom dashlets using the **Save As** feature. This will save the filter settings on a custom dashlet until you change and save different settings. Unlike the filters on the default dashlets, the filters you set on custom dashlets are persisted beyond the current Dashboard page session.

System settings: Dashlets that can be filtered by Platform reflect patches from the platform types applicable in your zone. For example, if the Linux platform is the only platform type selected for "platforms to download," then typically only patches from that platform will be shown or can be filtered in the dashlet.

One exception to the above statement is custom dashlets. Any applicable patches already downloaded before a change was made in the “platforms to download” would still be shown in applicable ‘custom’ dashlets if the excluded platform type was previously saved to show in the dashlet.

Patch dashlet descriptions: A brief description for each default dashlet is provided below. Click a dashlet link for more detailed information about that dashlet.

- Recently Released Patches: Displays the number of recently released patches by patch impact type. Mouse over different sections of the chart to see the number of patches for each impact type, or expand the dashlet for more options.
- Device Patch Compliance: Displays compliance status for devices in the zone. Mouse over different sections of the chart to see how many devices are compliant, or expand the dashlet for more options.

  NOTE: Patch compliance is measured by Critical and Recommended patch impacts, based on the percentage defined in the Dashboard and Trending configuration. Disabled patches for these impact types are not part of the compliance data.

- Device Last Patch Scan: Displays the number of devices scanned for patches by time range. Mouse over the chart to see the scan information, or expand the dashlet for more options.

Security dashlet descriptions: A brief description for each default dashlet is provided below. Click a dashlet link for more detailed information about that dashlet.

- Patch Tracker Dashlet: This dashlet is a unique dashlet when compared to other dashlets in ZENworks as it does not display any data by default. To view the data, the dashlet should first be configured. When you mouse over the dashlet, it displays the number of vulnerable devices against the total number of impacted devices for the selected patches. In the Vulnerability Trend section of the dashlet, you can view the vulnerability trend of the selected patches, for a specific time period.
- CVE Severity Distribution: Displays all the CVEs that are applicable to devices in the zone, grouped based on their severity. When you mouse over the dashlet you get to see the number of CVEs for each type of severity.
- Top CVEs : Displays the list of top CVEs in the zone based on the date on which they were released. However, you can use the filters to display the top CVEs based on the number of vulnerable devices or based on the severity. Mouse over different sections of the chart to see the number of vulnerable devices against the total number of impacted devices, for a particular CVE.
- CVE Tracker: The CVE Tracker dashlet also does not display any data by default. To view data, the dashlet should first be configured. When you mouse over this dashlet, it displays the number of vulnerable devices against the total number of applicable devices. In the Vulnerability Trend section of the dashlet, you can view the vulnerability trend of the selected CVEs, for a specific time period.

For general information about using the ZENworks Dashboard, see *Using the ZENworks Dashboard - An Overview*.

Recently Released Patches

By default, the Recently Released Patches dashlet displays all applicable patches discovered on devices in your Management Zone that were released in the last 30 days. Viewing the information in the default configuration might initially help you determine how to best configure the dashlet for your organization's needs by asking questions such as:

- What platform types do I need to patch?
- What patch impact types do I want to include?
- Do I want to see applicable patches from all vendors or just selected vendors in my dashboard?

From the expanded Recently Released Patches dashlet, you can configure the dashlet to only display those patches that you require to accurately assess your patch environment going forward. You can also create custom dashlets by saving the Recently Released Patches dashlet with another name.

Modify the data display: To filter the data that the dashlet displays, expand and modify any of the sections in the dashlet filter panel for Release Period, Platform, Impact, and Vendors, and then apply your changes.

Execute actions from the Patches panel: The Patches panel displays the patches that meet the criteria you define in the dashlet filter panel. You can also filter the list by searching for any portion of a patch name string via the **Search Patches** feature.

For information about other actions and options you have in the Patches panel, see the following:

- **Remediate patches:** If you see a patch that you need that will not be picked up by your patch policy, you can start remediation of the patch directly from the Patches panel. To start remediating patches, select one or more patches in the list, and click **Remediate**.

  Step 1 in the remediation process opens. For information about using the Remediation wizard, see Deploying Patches Manually.

- **Disable patches:** To disable one or more patches, select them in the Patches panel and click **Disable**.

  NOTE: There is no confirmation of this action. Once you click **Disable**, the action is executed.

  To enable a disabled patch, go to the **Security > Patches** page, locate and select the patch, and click **Enable** from the Action menu.

- **Download patches:** To download one or more patches, select them in the Patches panel, and click **Download**. A green status icon indicates that the patch or patches are downloaded.
- **View patch information:** To view vendor details about a patch, click the patch name in the Patches panel. The Patch information page provides useful details about the patch and a link to the vendor site.
- **View patched or not patched devices:** To see which devices are applicable to which patches, click the applicable number link in the Patched or Not Patched column. This will list the devices that already have or need that patch, respectively. The list of devices will also include a link to the Summary page for each device in the list.
- **Sort the Patches list:** To sort the list alphanumerically by column criteria, click a column header. Clicking the column a second time will invert the order of the sort.

Device Patch Compliance

When expanded, the Device Patch Compliance dashlet provides a quick snapshot of how many devices are compliant and how many are not, both by the number of devices in the chart and by percentages in the Devices panel. You can modify the threshold that you want for patch compliance in the Dashboard and Trending configuration. For more information on this setting, see Configuring the Security Dashboard.

Modify the data display: To filter the data that the dashlet displays, expand and modify any of the sections in the dashlet filter panel for Status, Impact, Device Type, and Platform, and then apply your changes.

Viewing options in the Devices panel: The Devices panel displays compliance status for each device in your zone by percentage, based on the criteria you define in the dashlet filter panel and compliance criteria in the Dashboard and Trending Configuration. You can also filter the list by searching for any portion of a device name via the **Search Devices** feature.

To see specifically which patches are compliant for each device, click a percentage link in either the Critical Patches or Recommended Patches column for a device in the list, and the Patches page will open for that device.

Device Last Patch Scan

Checking the data in the Device Patch Last Scan dashlet can help you determine the health of your current patch environment. When expanded, you can compare the latest scan with information from other patch dashlets and even go directly to the Vulnerability Detection Schedule to modify scan times, if there is a need.

Modify the data display: To filter the data that the dashlet displays, expand and modify any of the sections in the dashlet filter panel for Time Ranges, Platform, and Device Type, and then apply your changes.

Viewing options in the Devices panel: The Devices panel displays the last scan date and the next scheduled scan time for each device.You can also filter the list by searching for any portion of a device name via the **Search Devices** feature.

For information about other actions and options you have in the Devices panel, see the following:

- **View detailed device information:** To see specific information about a device in the Devices panel, click the device name.This will open the Summary page for that device.
- **Modify the scan schedule:** To go directly to the Vulnerability and Detection Schedule in the Patch Management configuration, click the link in the **Scan Schedule Defined At** column for any of the devices in the Devices panel. From here, you can modify the zone schedule that checks for device vulnerability.
- **Sort the Devices list:** To sort the list alphanumerically by column criteria, click a column header. Clicking the column a second time will invert the order of the sort.

Patch Tracker Dashlet

The Patch Tracker dashlet enables you to track a single or multiple patches available in the Management Zone. By drilling into the dashlet, you view the current patching status of the devices and also view the patching trend over a defined date range.

You can customize the dashlet to best fit your needs, and create multiple custom dashlets if necessary.

By default, the Patch Tracker dashlet does not display any information, to view information in the Patch Tracker, you need to first configure the dashlet. By configuring the Patch Tracker dashlet, you can track a single patch or multiple, associated, patches.

For the specified patches you can view the current patching status of the devices. The dashlet displays the number of devices that are patched against the total number of applicable devices. After identifying the vulnerable devices, you can use the Deploy Remediation quick task to apply the patches on the devices. With the Patch Tracker dashlet you can view the updated status as devices are patched. In the Unpatched Device Trend section of the dashlet, you can view the patching trend of the selected patches, for a specific time period.

Accessing the Dashlet: In ZCC, click **Security** > **Patch Tracker**.

Configuring the Patch Tracker Dashlet

1. In the Patch Tracker Dashlet, click Configuration, and then click **Add/Remove**.
2. In Select Patches, select the required patches, and then click **OK**.
3. Specify a name for the dashlet and change the tracker icon, if required.
4. Vertica is required to retrieve the trending data. Hence, the Trend Chart fields are enabled only when Vertica is configured

   In the Trend Chart section, based on your requirements, using the following option, you can assess the patch trending status in your Management Zone:

   a. **Date Grouping:** You can group the trend data based on Day, Week, Month, Quarter or Year.

      The chart will not be display any data until the end of the first period of the date grouping.

      Example: If you choose Year, then you will not see any Trend Chart data for a year. Hence, while creating a new tracker, ensure that you set the Date Grouping to Day so that you see the data immediately. You can modify the filter at a later time, if you want.

   b. **Date Range:** After selecting the Date Grouping filter, this option enables you to select the date range for the selected date grouping.

NOTE: Vertica is required to retrieve the trending data. The Trend Chart fields will be enabled only when Vertica is configured. For more information, see Vertica Database Reference.

5. Click Apply.
6. To save the dashlet, click the hamburger menu, and then select Save As.

After configuring the Patch Tracker dashlet, following information is displayed:

Patch Status: The Patch Status section provides current known status about the number of patched and unpatched devices that are grouped by platforms. Hover over each of the graph elements to know the number of patched and unpatched devices.

The number displayed in the Patch Status section represents the number of unpatched devices in the zone. The Patch Status graph is grouped based on platforms. This also displays the number of devices that are not patched in the Management Zone.

The Patch Status also displays an arrow that indicates the current unpatched device trend in the Management Zone. The following table describes the various scenarios and the associated status arrow:

- The green arrow pointing downwards represents the number of unpatched devices at the current point in time is less than the number of devices at the start of the date grouping period (Day, Week, Month, Quarter, or Year).
- The red arrow pointing upwards represents the number of unpatched devices at the current point in time is more than the number of devices at the start of the date grouping period (Day, Week, Month, Quarter, or Year).
- The two-sided arrow represents the number of unpatched devices at the current point in time is same as the number of devices at the start of the date grouping period (Day, Week, Month, Quarter, or Year).

Unpatched Device Trend: The trend chart displays the current and historical data of selected patches based on the selected date grouping and date range. By analyzing this section, you can check the patch trend in your zone and also take necessary actions, such as Deploy Remediation, to make your zone more secure. The trend data is displayed based on the server time.

NOTE: If a new device is added to the zone, then the trend data for the newly added device will be displayed only after the data is retrieved from Vertica. By default, the data from Vertica will be retrieved after 12 PM (Server Time).

For example, if the Date Grouping is Day and the Date Range is 1 Month, then the Unpatched Device Trend chart displays the trend for the last 30 days with each day represented as a point in the chart.

NOTE: The Unpatched Device Trend chart is displayed only when Vertica is configured and enabled. For more information, see the Vertica Database Reference in the documentation site.

Filtering the Dashlet Based on requirements, you can narrow-down the data displayed in the dashlet by using the Filter tab. Following are the available filter options:

- **Device Folders:** In this filter, you can select the required device folders. Select **Include Subfolders** to include folders within the selected folders.
- **Device Groups:** In this filter, you can select the required device groups.
- **Device Type:** In this filter, you can select the required type of device. The available options are Servers, Workstations and Mobile Devices.
- **Platform:** In this filter, you can select the required platform. The available options are Windows, Linux and Mac.
- **Vulnerability Status:** In this filter, you can select the vulnerability status of the device. The available options are Vulnerable or Not Vulnerable.

Execute actions from the Device Details panel

The Device Details panel displays the devices that meet the criteria that you defined in the dashlet filter panel. You can also filter the list by searching for a device name or a portion of the name in the search panel.

Following are the information displayed in the Device Details panel:

Field	Description
Device	Displays name of the device.
Status	Displays the vulnerability status of the device.
Last Vulnerability Scan	Displays the date and time at which the Vulnerability Scan was performed on the device.
Operating System	Displays operating system on which the device is operating.
Device Folder	Displays the folder path in which the device is located.
Remaining Vulnerabilities	Displays the number of vulnerabilities that should be applied on the device to make the device less vulnerable.

For information about other actions and options you have in the Device Details panel, see the following table:

Table 4-1 *Device Details Panel*

Task	Description
Deploy Remediation	Deploys all patches required to remediate the vulnerability on the selected devices. Any required patches that have not already been downloaded (cached) to your zone will be automatically downloaded. For more information, see Deploying Patches Manually.
Scan Now	This action initiates a patch scan on the selected devices in order to ensure that you have the latest vulnerability status for the devices.
Search	The Search operates on the Device, Operating System, and Device Folder fields to allow you to filter the list based on the data in those fields.

NOTE: For information about the other Security dashlets, see the Determine Vulnerabilities and Deploy Remediations section in the CVE Reference.

Viewing Patch Policies

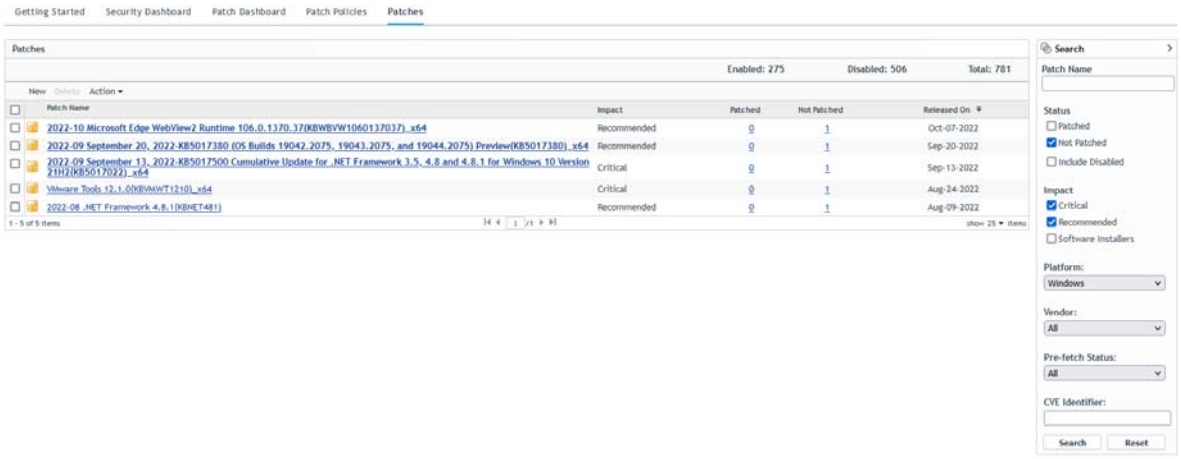
You view, create, modify, and delete patch policies from the Patch Policies page. For detailed information about creating and managing patch policies, see Creating and Publishing Patch Policies.

To view patch policies, navigate to **Security** > **Patch Policies**.

Viewing Zone Patches

To view the patches that are applicable to devices in your zone, click **Security** in the navigation menu, and select the **Patches** page.

The Patches page displays all patches that the Patch Agent has detected on your managed devices. The Patched column shows the number of devices on which the patch is installed and the Not Patched column displays the number of devices on which the patch is not installed.



Viewing Patch Status

The **Patch Download Details** page displays the download status for patches and bundles in table form, and also displays the details of patch caching and queuing status.

To view the Status page, navigate to **Security** > **Patch Download Details**.

The page consists of two data tables, **Patch Download Details** and **Cache Status**. Definitions for each table item are provided below:

Table 4-2 *Status Item Definitions*

Item Name	Item Status
Signature Download	Indicates whether downloading of the signature has finished or is in progress.
Signature Download Time	Indicates the last time the local server contacted and downloaded the signature from the Patch Subscription server.
Bundle Download	Indicates whether the patch bundle download is finished or is in progress.
Last Patch Download	Indicates the last time the local server contacted and downloaded a patch from the Patch Subscription server.
Number of Failed Download(s)	Indicates the number of patches that failed to download from the Patch Subscription server.
Number of Patches Queued for Caching	Indicates the number of patches that are queued for download from the Patch Subscription server.
Number of Active Patches	Indicates the number of patches that are available for download from the Patch Subscription server.
Number of New Patches (less than 30 days)	Indicates the number of patches that have been uploaded to the Patch Subscription server in the last 30 days and are available for download.
Latest Patch Released On	Indicates the time when the latest patches were released.

Table 4-3 Cache Status Item Definitions

Item	Definition
Action > Cancel Pending Downloads	Cancels the download of any patches in the process of being cached.
Name	The name of a patch.
Status	Whether the patch has been successfully downloaded.
Error Detail (if any)	Details of any error that occurred during the download process.

NOTE: By default, the SendChildPatchBundleStatus flag is enabled, i.e. the agent will upload the child patch bundle status to the server even if the registry is not created. Uploading child patch status to the server causes additional overhead on the server to process the status of child patch bundles also overhead on the agent to upload the status of child patch bundles.

If you want SendChildPatchBundleStatus to be disabled, then set the following registry to false:

SOFTWARE\\Novell\\ZCM\\SendChildPatchBundleStatus

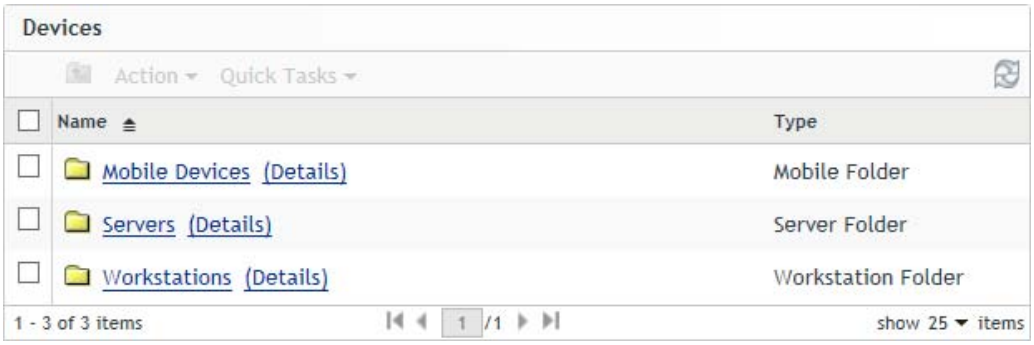
Viewing Patches for a Device

Device patches are the patches associated with a selected device (a server or a workstation). The patches listed for a specific device are the ones that are applicable only for that device. The following sections describe device patch information for ZENworks Patch Management:

To view the patches for a specific server or workstation device:

1 Click Devices in the navigation menu.

A page displaying the root folders for each type of device appears:



The Servers folder is the root folder for all managed servers and the Workstations folder is the root folder for all managed workstations.

2 Click the Servers or Workstations link.

A list of server or workstation groups classified on the basis of their operating systems appears.

Any of the following device icons might appear on the Servers or Workstations page:

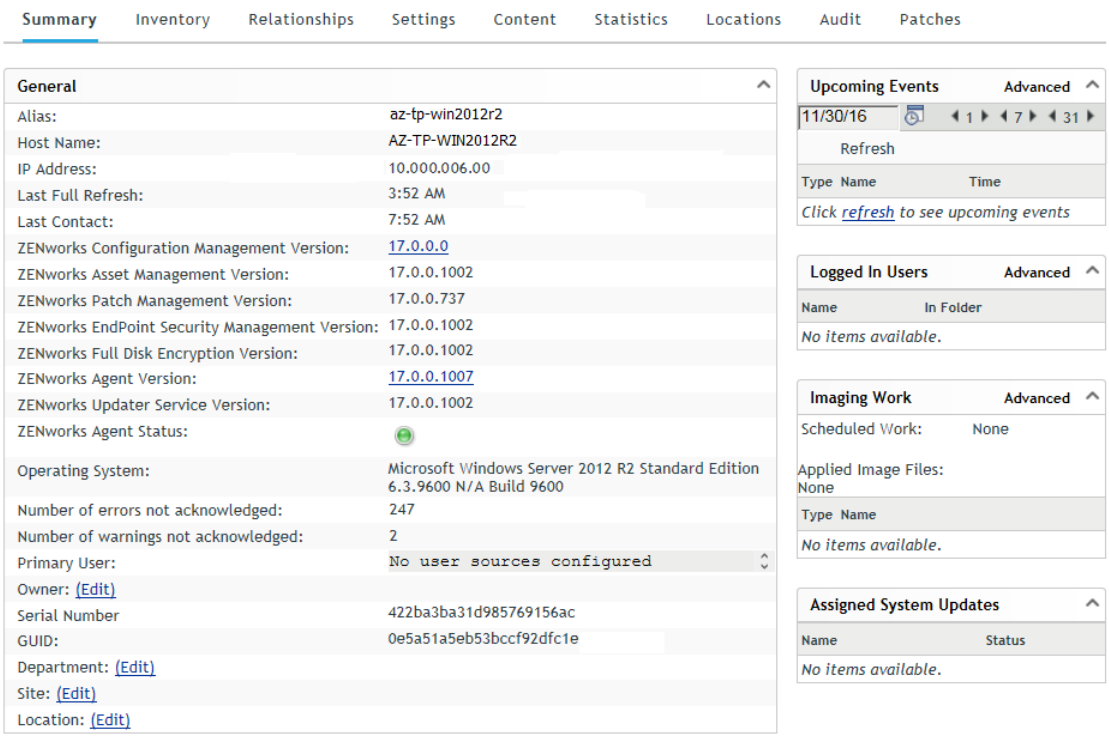
Icon	Status
	Message Status: Normal Device Status: Bundle and policy enforcement successful
	Message Status: Warning Device Status: Bundle and policy enforcement successful
	Message Status: Error Device Status: Bundle and policy enforcement successful
	Message Status: Error Device Status: Bundle and/or policy enforcement failed on one or more bundles or policies.

A specific device, type of device, or device with a given status can also be found using the Search feature on a group page. The following filters are available:

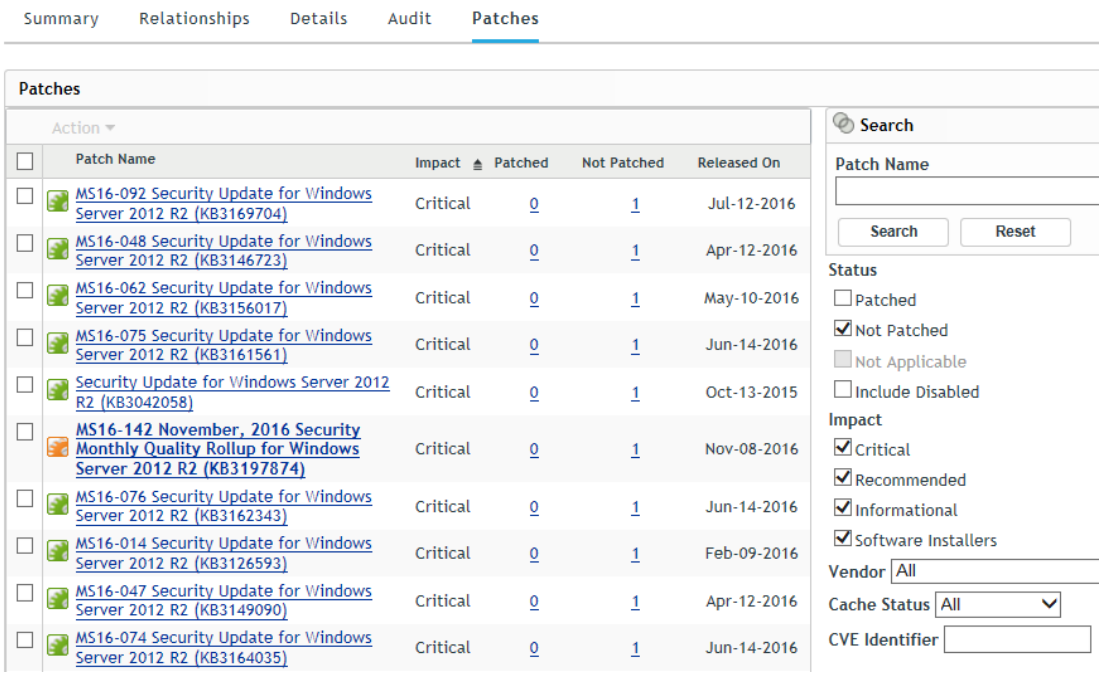
Filter Item	Result
Name	Searches for devices with a particular name.
Type	Searches for devices of a specific type or group.
Operating System	Searches for devices running a particular operating system.
Test Status	Searches for devices based on its ZCM test status.
Message Status	Searches for devices that display a particular message status.
Compliance Status	Searches for devices based on their compliance status, **Yes** or **No**.
Device Status	Searches for devices based on the device status.
ERI Status	Searches for devices using disk encryption based on ERI status, **Yes** or **No**.

3 Click a required group (Server, Dynamic Server, Workstation, Dynamic Workstation Group) to view details of the group and the members of the group. Alternatively, you can click a managed device in the group.

If you click a managed device, a page displaying details about the managed device or member is displayed, as shown in the following figure, where the name `az-tp-win2012r2` for the managed device is an example. The network administrator decides the name of the managed device.



4 Click the **Patches** page (either from a group or device page) to display the patches associated with the group or device:



Accessing Patch Management Reports

Reports are available to customers who install ZENworks Reporting Services (ZRS) inside ZENworks. Login to the ZENworks Reporting console to view the reports. For information on how to deploy or upgrade the ZENworks Appliance, see the *ZENworks Reporting Appliance Deployment and Administration Reference*.

- "Viewing Predefined Reports" on page 53
- "Generating Patch Audit Reports" on page 54
- "Common Patch Management Reports" on page 55

Viewing Predefined Reports

The following predefined reports are included for Patch Management:

- **Bundle Deployment Summary:** Displays only the devices on which the patch bundle have been deployed. This report lists deployment name, patch name, assigned device name, and patch device status.
- **Critical Patch Status Report:** Displays information on critical patches that are assigned to the devices. This report displays the total summary of the patch status and lists patched, not patched, not applicable, error, and total devices.
- **DAU Status:** Displays a pie chart that shows how many days since the Discover Applicable Updates (DAU) task was run on agents in the management zone (those greater than 7 days and those from 1-3 days).

- **Device Patch Status by Vendor:** Displays information on device patch status. This report lists agent name, vendor, patched, not patched, not applicable, released on, is patch enabled, and patch impact.
- **Device Status:** Displays a date-time stamp by device name for the following status indicators: Last Contact Date, Last Full Refresh, Last Inventory Scan, and Last DAU.
- **Not-Patched Patches by Device:** Displays a table for each device in the management zone that shows patches by the patch name, release date, impact, and vendor.
- **Overall Patch Percentage:** Displays the total number of devices, Patched and Not Patched, with their respective percentages. The percentages are also reflected in a pie chart.
- **Patch Analysis:** Displays information on patch assigned as mandatory baseline on a device. This report lists vendor, patch name, released date, criticality, applicable, patched, not patched, and % patched.
- **Patch Assessment Report:** Displays information on all released patches and their impact. This report lists vendor, released patches, and patch impact.
- **Patch Bundle Deployment Status:** Displays information on all released patch bundles and their status. This report lists administrator initiated remediation bundle, deployed patch bundle, event type, and event status.
- **Patch Deployment Summary:** Displays information on all released patch bundles and their status. This report lists admin initiated remediation bundle, deployed patch bundle, event type, and event status.
- **Patch Detail Report:** Displays detailed information on patches. This report lists patch name, patched status, total devices, and % patched.
- **Patch Percentage by Folder:** Displays the number of devices patched and not patched in each folder with a percentage of those not patched.
- **Patch Release Report:** Displays information on released patches. This report lists, patch device status, and device name.
- **Patch Tuesday Report:** Displays information on Tuesday's released patches. This report lists, patch name, patch status, and total devices.
- **Top 10 Not Patched Critical Patches:** Displays information on the most critical patches that are not deployed. This report lists patch name and patch impact.

Generating Patch Audit Reports

While not recommended for long term use due to database usage, two audit reports, Device Patch Audit and Patch Audit Summary, will be generated for patch deployments when the **Save patch status history** option is turned on in the Dashboard and Trending configuration. For information on how to deploy or upgrade the ZENworks Appliance, see the ZENworks Reporting Appliance Deployment and Administration Reference.

To configure the setting:

1. Go to **Configuration** > **Security** > **Dashboard and Trending** link.
2. In the Dashboard and Trending section, select the **Save patch status history (Warning: This can cause large database usage)** check box.
3. Choose the number of days to store the data in the database in the drop-down menu.
4. Click **Apply** at the bottom of the configuration page.

Common Patch Management Reports

To view list of patches that are due to be installed/assigned or to view the list of devices that are patched, you can create common reports. For more information, see Common ZENworks Reports in the ZENworks Reporting Universe Objects and Predefined Reports Reference.

5 Distribute and Apply Patches

There are two ways to distribute and apply patches to devices in the management zone:

- Create patch policies

  or

- Deploy patches manually

The first option automatically deploys patches based on rules and requirements you define in patch policies. The second option requires you to manually select the patches to deploy and manually configure their distribution. Both options require automated scans of devices to have a required patch list to draw from. Patches are installed according to the schedule in the applicable option, Patch Policy Settings or a remediation's Distribution Schedule.

While there are settings you can configure to pre-fetch and pre-cache patch content if required, by default, devices request patch content on-demand from their upstream Content Server in accordance with the scheduling referenced above. If the patch is not already available in the system at that time, an Ondemand Content Master downloads the patch and delivers it to the device through the Content Server stream. For more information see Understanding Pre-Fetching and Pre-Caching of Patches.

While using patch policies is the most efficient, preferred, and recommended way to manage patches, Deploy Remediation gives you the flexibility to quickly deploy patches, custom or otherwise, that may not be covered in your patch policies.

- "Understanding Pre-Fetching and Pre-Caching of Patches" on page 57
- "Creating and Publishing Patch Policies" on page 58
- "Deploying Patches Manually" on page 68
- "Deploying Patches on Mac Devices" on page 82

Understanding Pre-Fetching and Pre-Caching of Patches

Pre-fetching means that patch content is downloaded by an Ondemand Content Master (OCM) from external sources before it is requested on-demand by a device that has the Patch Agent installed. Pre-caching means that already fetched patch content is replicated to specified Content servers and Satellites in the ZENworks zone to make it more readily available when requested by devices.

A patch must be downloaded by an OCM before it can be cached. This could be a patch that the OCM downloaded on-demand because a device requested it, or it could be a patch that was pre-fetched because of the Pre-Fetching configuration settings. You must have at least one Primary Server designated as an OCM. When you configure the Patch Server, it is pre-selected by default as an OCM. However, by configuring one or more other Primary servers in the Server Hierarchy configuration as OCMs, you can remove the Patch Server as an OCM (if required). For information, see "Configure Ondemand Content Master Settings" in the *ZENworks Ondemand Content Reference*.

Rather than leaving the system default to only fetch and cache patches as they are requested on-demand by devices, you can configure zone settings to pre-fetch and pre-cache fetched content. Patches will continue to be pulled down on-demand by devices for installation by the Patch Agent according to the schedule set in Patch Policy Settings or in a remediation deployment. However, by configuring zone settings for pre-fetching and pre-caching, you can design the download and replication flow for content in a way that best suits your enterprise resources. For information about configuring content pre-fetch and pre-cache settings, see the following:

- Configuring Patch Pre-Fetch Settings
- Configuring Pre-Cached Content

Creating and Publishing Patch Policies

Patch policies are designed to make deployment of multiple patches easier across large estates. They can be used as a testing ground for new patches before they are released onto the network, and can also be used to filter content, so that some devices can be selected or omitted as part of the patch remediation.

Patch Policy - Best Practices

In general use, the Patch Policy function is the most effective and labor saving way to deploy patches across large estates. Once set up, it can deliver the patches to the target machines with much less oversight than manual remediation.

While we advocate the automated setup that this function delivers, it is important to remember not to overstretch your systems or the capabilities of the product.

Recommendations:

1. Keep the policies reasonably simple. Try to organize individual patch policies around a common outcome, for example: assuming some of your stock is comprised of Windows 10 machines; setup a policy called Win10 and use this to deliver all Microsoft updates to those targets. Similarly, you could organize policies by vendor or architecture.
2. Devise a naming convention for your policies; this will enable you to track policies more easily, and will also make it simpler to make changes to individual policies.
3. When you are setting up individual policies, try to plan into the policy. For example: in real terms, how often will a policy be deployed? does that specific vendor have regular updates? and what would your expectation be for throughput? It is our general recommendation that you should have a team process to steer your approach to this. This is in line with NIST recommendations.
4. When you are designing policies, be careful not to apply conflicting statements. There are a lot of different settings built in to ensure that policies can perform some very useful tasks, but be aware that changing Rules, Requirements, Actions, Relationships, and Members may bring your policy into conflict with previously defined settings.
5. Choose a schedule type based on network load, for example: it might be advisable to schedule policy deployments out of hours or at times when you know that your network will be least busy.
6. Use the Patch Policy Enforcement and Distribution settings in ZENworks > Configuration to their full extent, especially around Reboot settings; why reboot if the patch does not require this?

7. Use the Sandbox function to its full extent. We cannot stress how important it is to test patches before deploying them, especially over big networks. It is therefore prudent to set up a test server or a proving ground and deploy to this in the first instance. Once there has been a clean and issue free deployment, then you are ready to release to the wider network.

   For more information, see Test a Policy Before Deploying to a Live Environment.

8. Do not overload the policy. Patch Management has a default limit of no more than 1500 bundle actions per policy. This is to keep policies within a manageable parameter. If you believe your patch server has performance issues due to the number of patch bundle actions, you can divide up your patch polices with a more defined set of rules and requirements for each policy, which will reduce the number of actions per policy.

   You can also modify the default limit for policy bundle actions with the use of the system variable, PATCH_POLICY_ACTIONS_LIMIT. For information about setting the variable, see Patch Management System Variables.

9. Continually monitor patch policies, ensuring that you have the available space and bandwidth to avoid any calamity on your network. If you have large groupings among your assets, it may be necessary to stagger deployments; this way you will not impact the integrity of your network, and normal operating can continue alongside the task of protecting against future problems.

10. If you want to make changes to the schedule of a Patch Policy, ensure that you configure it within the Patch Policy Settings page. If the schedule is configured within any other page of ZCC, such as Device's Assignments or the Bundle's Relationship page, under Assignment Details, it will not override the schedule that was previously defined in the Patch Policy Settings page. Instead, it will be run multiple times, based on the schedule configured within each page.

11. If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of **Not Installed** for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

12. Vendors will occasionally supersede Critical patches with Recommended patches. For example, Microsoft sometimes releases a second recommended Windows 10 cumulative update later in the month that supersedes an earlier critical update. The recommended update fixes the same security issues as the superseded critical update, but no new security issues are fixed so Microsoft rates it as Recommended rather than Critical.

    If you want to continue to distribute the Critical patch rather than a Recommended patch that supersedes it, you can use the following options:

    - Delay the disabling of superseded patches for: This option causes the superseded patch to remain enabled so that it can continue distributed to devices.
    - Do not disable superseded patches that are included in a policy: This option keeps a superseded patch enabled until it is removed from a Patch policy during the policy's next scheduled rebuild.

    For example, assume that you have a Patch policy that installs all Microsoft critical patches. If Microsoft releases a second recommended monthly update that supersedes the critical monthly update, the superseded critical monthly update will no longer be distributed by the policy and the recommended update will not be included in the policy (even if the policy is rebuilt) because it is not critical. To avoid this situation and ensure that devices continue to receive the critical cumulative update, you would need to enable the "Do not disable superseded patches that are included in a policy" option.

A second example would be a Patch policy that installs all patches with “Cumulative Update for Windows 10” in the name. Occasionally, Microsoft releases a preview patch with “Cumulative Update Preview for Windows 10” in the name. The preview patch, which is recommended, supersedes the critical cumulative update so the policy no longer installs the superseded critical update. In this situation, enabling the “Do not disable superseded patches that are currently in a policy” option would also resolve the issue.

The two supersedence options are in the CVE and Patch Cleanup settings in ZENworks Control Center (**Configuration** > **Management Zone Settings** > **Security** > **CVE and Patch Cleanup**).

Create a Patch Policy

Before creating a patch policy it is important to plan your deployment, and ensure that you know the devices you would like to reach and the remediations you would like to deliver. It is recommended that you setup a test machine to test the efficacy of the patch before deploying across a global environment. For more information, see Test a Policy Before Deploying to a Live Environment.

To create a new patch policy:

1. Click **Security** in the navigation menu, and select the **Patch Policies** page.
2. Click **New** in the Patch Policies panel.
3. Choose a platform, and click **Next**.
4. Name the policy, add any descriptive notes to identify the policy by, and click **Next**.
5. Click **Add Filter** and select rules for the policy that will limit the patches cached in the zone to only those you need. The following filters are available:

Filter Item	Result
Age	Select by age of patch: in days, weeks, months etc.
Architecture	Toggle between 32bit and 64bit
CVE Identifier	Insert a relevant CVE code
Impact	Choose Impact of patch ‘Critical’ or ‘Recommended’. **NOTE:** Software Installers are not included to avoid unnecessary risk. However, you can always add specific installers to the policy via the Members tab. For more information, see Step 4 in Configure Advanced Parameters.
Patch Name	Filter by Patch Name ie: MSxxx xxx
Release date	Select by Patch Release date
Vendor	Select by Patch Vendor

   It is also possible to add multiple filters; by clicking **Add Filter Set**, you can add a number of extra levels to further refine the patch cadre. For example, you could filter by Age + Architecture + Vendor.
6. Once the selection is made, click **Apply**. The box below the selection tool will populate with relevant patches (assuming that you have replicated and have at least one registered agent).

Review the Patches in the Included Patches table, and if satisfied to continue, click **Next**.

7 In the next page configure the settings for the Patch Policy rebuild schedule and publish schedule as defined below:

Rebuild Schedule

The Rebuild Schedule determines how often you want the Patch Policy to rebuild. The build essentially refreshes the policy to include any patches matching rules that you set in the policy that have been released since the last build and delivers those patches to assigned devices. Building the policy without publishing enables you to install patches on Test devices before deploying the policy in your operational environment.

NOTE: In addition to the schedule you define here, you will have the option to build the policy upon creation rather than waiting for the first scheduled build; or, you can run a build manually at anytime after policy creation by navigating to the **Automation** page on a selected policy.

Configuration options for the build schedule are described below:

- ***Days of the week:*** This option enables you to schedule the build on selected days of the week.

  To set the build day, select the **Days of the week** button, select the required day or days of the week, and set the start time for the build.

- ***Monthly:*** This option enables you to specify the monthly build options.

  In the Monthly build option, you can specify the following:

  - **Day of the month:** Enables you to schedule the build on a specific day of the month. You can specify any number between 1 and 31.
  - **Last day of the month:** Enables you to schedule the build on the last day of the month.
  - **Particular days of the month:** Enables you to schedule the build on a specific day or days of every month. The valid options for the day are first, second, third, fourth, and fifth. The valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows.

    To select an additional day of the month, click the **Plus** icon and use the drop-down arrows in the second row. To remove a particular day from the list, click the **Minus** icon.

- ***Fixed Interval:*** This option enables you to schedule a recurring build that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date and time for the build schedule.

Publish Schedule

The Patch Policy does not get enforced on operational devices until it is published. However, we highly recommend that you test the policy in Sandbox mode before publishing to your live environment. For more information, see Test a Policy Before Deploying to a Live Environment.

Publish options are defined below:

- ***Do not publish:*** This option is the default setting for the policy and requires you to manually publish the policy, which you can do directly from the policy or from the **Action** menu with the policy selected in the Patch Policies page.
- ***Publish immediately:*** This option has no backstop for deploying the policy on Test devices and we recommend that you use it with caution.

- ***Publish after successful Sandbox version enforcement on __% of test devices:*** This option will publish the Patch Policy automatically after the percentage of test devices specified here is successfully patched. The default setting shown in a new policy subscribes to the percentage set in the **Patch Test Devices** configuration.
  - **Delay publishing for __ days after successful enforcement:** This option is only enabled if you select the parent option. Valid numbers are 0 through 90.

8 Configure the final options for creating the policy in Step 4 of the wizard (see below), and then click **Finish**.

Option	Description
Create as Sandbox	Enabled by default and strongly recommended in order to test the policy before deploying in your live environment. You cannot disable the setting unless you deselect the **Build policy on creation** option, which is also set by default.
Build policy on creation	Enabled by default. Builds the patch policy upon policy creation to deploy patches to assigned Test devices.
Define additional properties	Opens directly to the policy editing pages after the policy is created. From here you can assign the policy and make other property changes. When this option is not selected, the Patch Policies list displays, and you have to open the policy from the list to define additional properties. See Configure Advanced Parameters.

Before you can test or publish a policy, you need to assign one or more devices to it and then execute the Build function. Any changes to the patch policy after initially testing it, or publishing it, will not be effective until you either manually rebuild the policy or it is auto-rebuilt based on the schedule you set when creating the policy. Both the manual Build option and the Rebuild Schedule are accessible from the **Automation** page on a selected policy.

For information on editing a patch policy, assigning the patch policy to devices, testing the patch policy, or publishing the patch policy, see the following:

- Editing Patch Policies
- Assign a Patch Policy to Devices
- Test a Policy Before Deploying to a Live Environment
- Publish a Patch Policy

IMPORTANT: If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of **Not Installed** for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

Configure Advanced Parameters

To achieve an even more targeted remediation within the Patch Policy function, there are a number of advanced settings available. These settings are accessible when a patch policy is opened from the Patch Policies page or when **Define Additional Properties** is selected during patch creation.

To configure advanced parameters in a patch policy:

1. Go to **Security** > **Patch Policies**.
2. Click a patch name in the **Patch Policies** page to display the editing page options. In addition to the Summary and Relationships pages, there are six other pages where you can modify patch policy criteria:
   - Requirements
   - Rules
   - Members
   - Actions
   - Automation
   - Patches
3. Select the **Requirements** page to configure filters from several variables that further define the devices that will get patched as a result of the patch policy.

   Click **Add** to choose a single filter option, or click **Add Filter Set** to insert the and/or operator between a set of variables.

Filter Item	Result	Platform
Architecture	Toggle between 32bit and 64bit	All
Bundle Installed	Choose between installed bundles	All
Configuration Location	The location of the server	All
Configuration Network Environment	Select the network environment	All
Connected	Connected or Not Connected	All
Connection Speed	Choose the speed of the connection	All
Disk Space Free	Select by Disk space available	All
Disk Space Total	Select by Disk space total	All
Disk Space Used	Select by Disk space used	All
Environment Variable Exists	Is there a pre-existing variable	All
Environment Variable Value	The value of the pre-existing variable	All
File Date	Select by File date	All
File Exists	Select by pre-existing File name	All

Filter Item	Result	Platform
File Size	Select by File size	All
File Version	Select by File version	Windows
IP Segment	Select by pre-existing File date	All
Linux Distribution	Select the Linux variants to target	Linux
Linux Kernel version	Select the Linux Kernel version to target	Linux
Linux Service Pack	Select the Service pack version to target	Linux
Logged on to Primary Workstation	Select Logged on or not Logged on	Windows
Mac Distribution	Select the Mac OS version	Mac
Memory	Choose the memory	All
Novell Client Installed	Novell client installed - yes or no	Windows
Operating System- Windows	Choose the Windows variant	Windows
Primary User is Logged In	Primary user logged in -yes or no	Windows
Processor Family	Select by Processor	All
Processor Speed	Select by Processor speed	All
Registry Key Exists	Add a Registry Key and choose yes or no	Windows
Registry Key Value	Add a Registry Key value and yes or no	Windows
Registry Key and Value Exists	Add a Registry Key and Value and yes or no	Windows
Security Location	Select by security location	Windows
Service Exists	Insert a Service name and yes or no	All
Specified Devices	Add specific devices (has search function)	All
Version of Application	Select by Application Version	Mac
Version of RPM	Select by RPM Version	Linux
ZENworks Agent Version	Select by ZENworks Agent version	Windows

4 Select the Members page to add a specific patch to the policy.

The patches can be selected by Name, Impact, Date, Vendor, or All and either added or removed. If you are using this feature in conjunction with other settings, it will ensure no duplication of caching, and the selected patch will stay as a member of the policy until it is removed.

5 Select the **Actions** page to specify an administrative action before or after a deployment.

Click the **Add** button on Pre-Enforcement or Post-Enforcement sections to open the selection menu. Each selection has its own set of custom parameters.

End Process	Choose to end a process -i.e. Notepad
File Removal	Choose to remove a file
Install Bundle	Select to install a bundle
Launch Bundle	Select to launch a bundle
Launch Executable	Launch an executable
Run Script	Run a custom script

6 The purpose of the patches page is for the user to have control over the deployment of patches. When a policy is first created, the final step is to rebuild the policy. This is done using the **Rebuild** button on the policy Summary page. After this button is clicked, the list of patches in the Patches page should populate.

After the page is populated with patches, click **Actions** and it will open a small menu. The options available are **Enable, Disable**, and **Update Cache.** When you have an action to take, check the box next to the patch you wish to take action with and select the appropriate action. The Patches page also contains information about patch deployment status, including patch impact, patch or not patched devices for a given patch, and the patch release date.

Editing Patch Policies

Using the Edit option you can make a copy of or rename an existing patch policy. You can save time by copying a patch policy when a complex patch configuration can be reused or slightly modified. The selection box must be checked to enable this option. When you copy a patch policy, the published version of the policy is copied.

Assign a Patch Policy to Devices

Once a patch policy is created and configured, you need to assign it to one or more devices. You can also assign it to a workstation group. If you have not already configured one or more devices as Test devices, see Test a Policy Before Deploying to a Live Environment.

To assign a patch policy to one or more devices:

1 Go to the Patch Policy Summary page (**Security** > **Patch Policies**), and click the patch link in the Name column.

2 Select the **Relationships** page, and click **Add**.

3 Click the down arrow for **Devices** to display the type of devices available.

4 Click the down arrow for **Servers** or **Workstations** to display the groups and devices for the selected folder.

5 Select the devices that are targeted for patch testing or deployment to move them into the **Selected** panel, and then click **OK**.

IMPORTANT: If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

The devices assigned to the patch policy will now be listed in the Relationships page. With the assignment complete, you are ready to test and publish the policy.

Test a Policy Before Deploying to a Live Environment

We advise ZENworks Administrators to always dry run their policies on a Test device before releasing to a live environment. Once a policy is released in a live environment, rescinding the changes that have been made can be difficult and time consuming.

Normally you would configure your Test devices before creating a patch policy for them; however, you can run a Rebuild at anytime. The Rebuild command uses the Sandbox to apply patches on all test devices assigned to the policy that is being rebuilt, according to the rules you configure for the policy.

If your test devices are configured as "Test" devices before they are assigned to the patch policy, applicable patches are automatically deployed to the test devices without rebuilding or publishing.

Publish after successful Sandbox version enforcement

If the patch policy has **Publish after successful Sandbox version enforcement** configured, the policy will automatically enforce on non-Test devices assigned to the policy after successfully applying ALL patches to the percentage of Test devices specified in this setting.

Other considerations for this setting:

- A patch scan determines and reports when the specified percentage of Test devices assigned to the policy have all applicable patches installed.
- Having any of your assigned test devices offline for an extended period of time could impact the timing of non-Test devices assigned to the policy from getting patched.
- Rebuilds (whether manual or automatic from the Rebuild Schedule), that are spaced too close together, could impact the timeliness of patching, because a rebuild restarts the patching of any uninstalled patches on Test devices according to the schedule set in the patch policy.
- Once all assigned Test devices are successfully patched, the patch policy is published, irrespective of any schedule settings. However, when **Publish after successful Sandbox version enforcement** is enabled, you can use the **Delay publishing** option in the policy Schedule page to delay this action.
- Patches are not applied to any devices (Test or non-Test) until the ZENworks Agent is refreshed on applicable devices.

To configure one or more devices for Test:

1. Beginning in the navigation menu, click **Devices** > **Workstations**.
2. Select the check box for one or more devices. Only workstations or Satellites can be configured for test, a Primary Server cannot be used for testing while operating as a server.
3. Open the **Action** drop-down menu, and select **Set as Test**.

   Once you have made the selection, a small yellow arrow appears on the workstation icon . If you mouse over the workstation icon, an info box displays “Test Workstation.”
4. If you assigned the test device(s) to the policy before configuring it as a test device, you can now execute the **Build Now** option from the policy Automation page to test the policy. Otherwise, make the assignments before testing the policy.

NOTE: You can also configure devices for testing directly from the device Summary page by clicking the **Set** link on the **Test Device** item. However, you can only configure one device at a time in this manner.

Configuring the Success Rate for Patch Test Devices

When deploying a Patch Policy in a test environment, which is strongly recommended, you can configure the policy to automatically deploy to your live environment once the success rate percentage you define in the **Patch Test Devices** configuration is met. This configuration defines the default value shown in a patch policy when creating the policy. However, you can change the default value when creating the policy or anytime thereafter in the Policy > Schedule page.

The default setting in the Patch Test Devices configuration is 100 percent. To change the default setting, navigate to Configuration > Management Zone Settings > Security > Patch Test Devices.

For information about this setting in the Patch Policy, see the **Publish Schedule** settings, in the Create a Patch Policy section.

Publish a Patch Policy

If you chose to not **Publish after successful Sandbox version enforcements** in the patch policy configuration, you will need to publish the policy after executing Build to apply patches to policy-assigned devices that are not set as Test devices.

To publish a patch policy:

1. Go to the Patch Policy Summary page, **Security** > **Patch Policies**, and click the patch link in the Name column.
2. Review the policy configuration in the Summary page (if applicable, make changes).
3. Select the **Automation** tab and click **Build Now**.

   When the policy is first created, its default status is **Sandbox** in the Displayed Version menu at the top of the page. If the policy was previously published, it will have one or more policy versions to choose from here.
4. Click **Publish** to update the information in the summary box and to publish the policy.

   If you return to your agent device and refresh it, you will see the policy in the ZENworks Agent window.

IMPORTANT: If you delete an old patch policy from an end point and then publish a new policy to replace it, the end point may list a Device-Assigned Bundle Status of Not Installed for an indefinite period of time. If you encounter this end point status, reboot the end point to complete publication of the patch policy.

Deploying Patches Manually

To distribute patches manually, use the Deploy Remediation Wizard, which provides an interface to create or edit patch deployment schedules for multiple recipients or devices. The wizard assists in selecting devices, scheduling deployment of patches, and if required, setting recurrence. After completing the wizard, the deployment will be listed in the Bundles page.

NOTE: To deploy a Windows patch, it is recommended that the minimum disk space required is at least 5x the largest available patch. If you are deploying multiple patches, then the minimum disk space required is at least 5x the total size of the patches.

You can access the Deploy Remediation Wizard from the Action menu on one of the following pages:

- Security > Dashboard > Recently Released Patches
- Security > Patches
- Devices > [selected device] > Patches

You can also click the **Deploy Remediation** link under Patch Management shortcuts in the navigation menu. These shortcut options appear when the Patch Management > Patches page is open.

If you select multiple patches in the Deployment Remediation Wizard, the wizard automatically selects all the applicable devices and packages. If any device is selected, the wizard automatically selects all patches that are applicable for that device. If a group is selected, the wizard includes all patches applicable for the devices in that particular group.

IMPORTANT: Once you initiate a patch remediation and the patch bundles are created for the remediation, the patch bundles should not be modified. If patch remediation bundles get modified, they may not replicate to Primary servers leaving the intended devices not patched.

Create a Deployment Schedule

To create a deployment schedule for one or more patches on one or more devices:

1. Go to **Security** > **Dashboard** or **Security** > **Patches**.
2. Select one or more patches that you want to deploy.
3. Select **Deploy Remediation** in the **Action** menu.

The Deploy Remediation steps vary, depending on the remediation option chosen in Step 5 of the wizard, **Default** or **Custom**. For information about a specific step, click its applicable link in the table below:

Deploy Remediation Steps		
Auto Reboot	**No Reboot**	**Advanced**
1. Confirm Devices 2. Remediation Schedule 3. Deployment Order and Behavior 4. Remediation Options 5. Notification and Reboot Options 6. Choose Deployment Name 7. Deployment Summary	1. Confirm Devices 2. Remediation Schedule 3. Deployment Order and Behavior 4. Remediation Options 5. Choose Deployment Name 6. Deployment Summary	1. Confirm Devices 2. Remediation Schedule 3. Deployment Order and Behavior 4. Remediation Options 5. Pre-Install Notification Options 6. Distribution Schedule 7. Notification and Reboot Options 8. Choose Deployment Name 9. Deployment Summary

Confirm Devices

The Confirm Devices page allows you to select and confirm the devices for which you need to schedule a deployment.

The page indicates the total number of devices to which the selected patch will be deployed. You can change how many items are listed on the page by using the **show items** drop-down menu.

1 Select one of the following options to determine the devices to which the patches are to be deployed:

- **All non-patched devices:** Deploys the patch to those devices that are in a non-patched state. Selecting this option deploys the patch to all the devices that are not patched.
- **Select applicable devices:** Deploys the patch to the devices you select from the devices list. You can deploy a patch to a device regardless of its existing patch status, which can be patched or not patched.

  NOTE: If you deploy a patch from the Patch Management page, the list of devices that appears is based on the patch **Status** filter you choose.

Column Heading	Description
Device Name	The name of the device. The name of the device registered with ZENworks Patch Management to which the patch is to be deployed.
Last Contact	The status of the device when they were last contacted.
Platform	The operating system of the device.
DNS	The name of the DNS server.
IP Address	The IP address of the device.

- **Select devices, folders and groups:** Deploys the patch to specific devices, folders, or groups that are in a non-patched state.

  To select a device, folder, or group for deployment:

  1. Click the **Add** menu item on the Confirm Devices page.
  2. Click the arrow next to the **Devices** option on the left side of the window to display the available devices, folders, and groups.
  3. Click the desired device to add it to the **Selected** panel on the right side of the window.

     or

     To remove a device from the panel, click the **Delete** button in the **Remove** column for that device.
  4. Click **OK** to confirm device selection.

     The window closes and the Confirm Devices page displays the selection.

2 After choosing an option and selecting one or more devices, click **Next** to open the Remediation Schedule page.

Remediation Schedule

In the Remediation Schedule page you configure how a patch is scheduled and deployed for selected devices.

To start setting the remediation schedule, you need to select the schedule type. Patch Management offers three types of schedules to determine when the patches are actually applied to the target device, Now, Date Specific, and Recurring:

- **Now:** Schedules the deployment to your selected devices immediately after you complete all the steps in the Deployment Remediation Wizard.
- **Date Specific:** Schedules the deployment to your selected devices according to the selected date.

  When you select **Date Specific**, you can choose from the following schedule options:

  - ***Start Date:*** Enables you to pick the date when you need to start the deployment. To do so, click the plus icon ⊞ to open the calendar and pick the date. To remove the selected date, click the minus icon ⊟.

- ***Run event every year:*** Ensures that the deployment starts on a selected date at a selected time, repeats every year, and if defined, ends on a specific date.
- ***Process immediately if device unable to execute on schedule:*** Ensures that the deployment starts immediately if the device could not execute on the selected schedule.
- ***Select when schedule execution should start:*** There are two options to enable you to select the start time of the schedule execution using a 24 hour clock, namely:
  - **Start immediately at Start Time:** Deactivates the **End Time** panel and starts the deployment at the start time specified. In this option, you must set the start time in the **Start Time** panel:

  - **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at a random time between them. The **End Time** panel appears as follows:

  Selecting the **Use Coordinated Universal Time** check box enables you to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at the local time.

- **Recurring:** Starts the deployment on the selected day at a selected time, repeats the deployment every day/week/month, and if defined, ends on a specific date.

  By default, the bundle install frequency is set to **Install once per device.** For a recurring deployment, change it to **Install always**, after finishing the Deploy Remediation Wizard. For more information, see "Install Action Set Options" in the *ZENworks Software Distribution Reference*.

  In the Recurring Remediation Schedule, you can set the following options for a recurring deployment:

  - ***When a Device is Refreshed:*** This option enables you to schedule a recurring deployment whenever the device is refreshed. In this option, you can choose to delay the next deployment until after a specific time.

    To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time to delay the deployment:

    NOTE: The device is refreshed based on the settings in the **Device Management** page under the **Configuration** page. Click the **Device Refresh Schedule** link under **Device Management** to open the page displaying the option for either a **Manual Refresh** or **Timed Refresh**. Alternatively, you can refresh the device by selecting a device under the **Devices** page and clicking the **Refresh Device** option under the **Quick Tasks** menu.

  - ***Days of the Week:*** This option enables you to schedule the deployment on selected days of the week:

To set the day of deployment, select the **Days of the week** button, select the required day of the week, and set the start time of deployment. If you click the **More Options** link, additional deployment options appear:

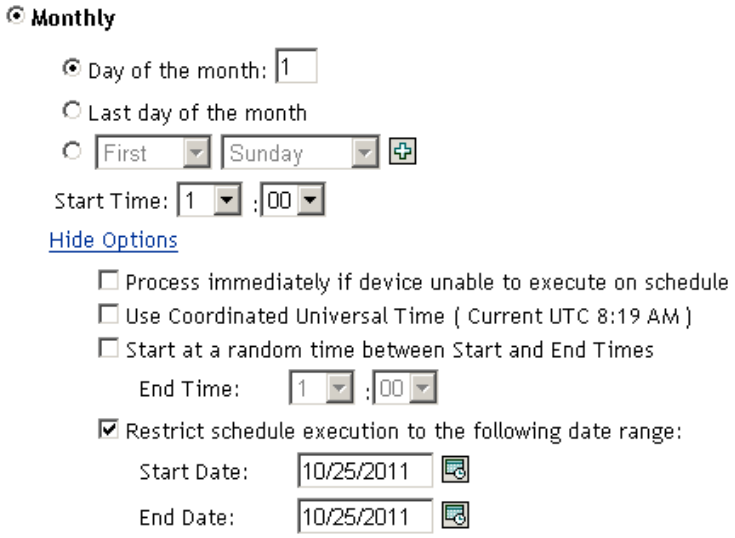
- Select the **Use Coordinated Universal Time** check box to schedule the deployment of all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.
- Select the **Start at a random time between Start Time and End Times** check box to activate the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the deployment occurs at any random time between the start and end times.
- The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and if defined, end at the specific time. This option also enables you to restrict the deployment to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

- ***Monthly:*** In the **Monthly** deployment option, you can specify the following:
  - **Days of the month:** Enables you to schedule the deployment on a specific day of the month. You can specify any number between 1 and 31.
  - **Last day of the month:** Enables you to schedule the deployment on the last day of the month.
  - **Particular days of the month:** Enables you to schedule the deployment on specific days of every month. The valid options for the day are first, second, third, fourth, and fifth. The valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows. An example is shown as follows.

To select an additional day of the month, click the **Plus** icon and use the drop-down arrows in the second row.

To remove a particular day from the list, click the **Minus** icon.

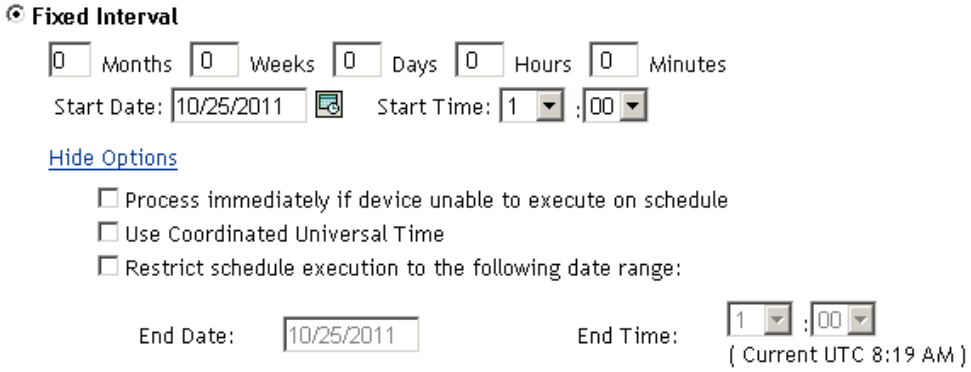
If you click the **More Options** link, additional deployment options appear as shown below.



NOTE: The **Restrict schedule execution to the following date range** option enables you to schedule a recurring deployment at the selected time, repeat the deployment on the days specified, and if defined, end on the specific time. This option also enables you to restrict the deployment to the period between the Start Date and the End Date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the **Time** icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

- ***Fixed Interval:*** This option enables you to schedule a recurring deployment that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the deployment schedule.

  If you click the **More Options** link, additional deployment options appear:



By default, the Device Refresh Schedule is set to twice a day. For testing and demonstration purposes, you could increase the frequency to once every five to fifteen minutes.

All of the schedule settings above also have the option to configure the Wake-on-LAN setting, which can schedule a deployment to devices that are powered off. For more information, see Remediation Schedule: Wake On LAN.

Remediation Schedule: Wake On LAN

The Wake on LAN function is an option in Remediation schedule. It can be used to set a deployment even if the managed devices are powered off. The parameters can be changed by pressing the (options) button, where you can select different servers for the wake up request and wake up broadcast.

NOTE: The default settings for this function are to automatically detect the Primary Server.

To change the parameters:

1. Select the **Wake On LAN** check box.
2. Click **Options**. This opens the Wake Up window.
3. Select the desired parameters, and click **OK**.

Deployment Order and Behavior

The Deployment Order and Behavior page enables you to set the order for each deployment schedule by two prioritized lists, Vendor Patches and Custom Patches. Vendor patches, if present, will always deploy first, followed by any custom patches. If you have more than one patch in either list, use the arrow buttons to set the priority for deployment.

Each list consists of the following:

- **Patch Name:** The name of the patch that has been selected for deployment.
- **Order:** The order of execution of the deployment. The arrow appearing next to the column heading enables you to sort in ascending or descending order.
- **Reboot:** The reboot settings applicable for the corresponding patch.

NOTE: Chained patches can be moved only after removing their chained status.

Click **Next** to open the Remediation Options page.

Remediation Options

The Remediation Options page enables you to select the required remediation option for each deployment schedule.

The following table describes the configuration for each option available in the Remediation Options page:

Table 5-1 *The Remediation Options*

Remediation Option	Functionality
Auto Reboot (silent install with optional reboot)	Automatically sets all possible patches to deploy with QChain enabled. Enables you to configure notification and reboot settings defined for each patch.
No Reboot (silent install, never reboot)	Automatically sets all possible patches to deploy with QChain enabled. All necessary reboots must be performed manually.
Advanced (individually set all possible deployment options)	Enables you to customize the following settings for the selected patch or patches: ◆ Pre-Install Notification Options ◆ Distribution Schedule ◆ Notification and Reboot Options

Pre-Install Notification Options

The Pre-Install Notification Options page allows you to define whether users receive any notification when patches are downloaded and installed, and to customize the notification. This page is only shown if you have selected the Custom remediation option in Step 5 of the wizard.

NOTE: The **Pre Install Notification Option** only displays if the **Advanced** option is selected in **Step 5: Remediation Options**.

Refer to the information below to understand how to define Pre Install options:

- **Use values assigned to system variables or defaults:** Select this option to use the default pre-install notification options defined within **Patch Policy Settings.**
- **Override Settings:** Select this option to override the default options and choose new ones. Selecting this option makes the remaining options available.
  - ***Notify Users of Patch Install:*** Select this option to notify the user prior to the installation of the patch. There are two additional options:
    - **Prompt before download:** Select this option to notify the user when the patch download process begins.
    - **Prompt before install:** Select this option to notify the user when the patch installation process begins.
  - ***Description text:*** The text of the notification message. You can edit this field only if you override the default settings.

- ***Options:*** When you define installation options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or the custom settings. There are three options:
  - **Allow User to cancel:** Allows the user to cancel the patch installation.
  - **Allow User to snooze:** Allows the user to delay the installation.
    - **Snooze interval:** The duration the install is delayed when the user snoozes.
    - **Install within:** The deadline that the user can no longer snooze the installation.

    NOTE: Even if you snooze the installation, the popup window will continue to appear every few seconds until you proceed with or cancel the installation.
  - **Show tray notification:** On selecting this option, a notification for a pending installation is displayed in the system tray. If you select this option, define the following:
    - **Tray notification duration:** Enter a value in hours, minutes or seconds for how long the system tray notification is displayed before being hidden.
    - **Tray notification text:** Type the text you want to appear in the notification.

Click the **Next** button to proceed to the Notification and Reboot Options Distribution Schedule page.

Distribution Schedule

The Distribution Schedule page of the Deploy Remediation Wizard allows you to determine when a patch will be distributed to and installed on the devices. This page is only shown if you have selected the Custom remediation option in Step 5 of the wizard.

To start setting the distribution schedule, you need to select the schedule type. Patch Management offers three types of schedules to determine when the patches are actually distributed to the target device: No Schedule, Date Specific, and Recurring.

- **No Schedule:** If you select **No Schedule**, the distribution to your selected devices begins immediately after you complete all the steps in the Deploy Remediation Wizard.
- **Date Specific:** If you select **Date Specific**, the distribution to your selected devices occurs according to the selected date that you set in the wizard's Distribution Schedule page, as follows:
  - ***Start Date:*** Enables you to pick the date when you need to start the distribution. To do so, click the plus icon to open the calendar and pick the date. To remove the selected date, click the minus icon.
  - ***Run event every year:*** Ensures that the distribution starts on a selected date at a selected time, repeats every year, and if defined, ends on a specific date.
  - ***Process immediately if device unable to execute on schedule:*** Ensures that the distribution starts immediately if the device could not execute on the selected schedule.
  - ***Select when schedule execution should start:*** There are two options to enable you to select the start time of the schedule execution namely:
    - **Start immediately at Start Time:** Deactivates the **End Time** panel and starts the distribution at the start time specified. In this option, you must set the start time in the **Start Time** panel:

- **Start at a random time between Start Time and End Times:** Activates the **End Time** panel next to the **Start Time** panel. You can specify the end time and the start time so that the distribution occurs at a random time between them. The **End Time** panel appears as follows:

In both time panels, the first drop-down list enables you to select the hour, the second drop-down list enables you to select the minute, and the third drop-down list enables you to select **am** and **pm**.

Selecting the **Use Coordinated Universal Time** check box enables you to schedule the distribution to all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at the local time.

- **Recurring:** If you select **Recurring**, you can start the distribution on the selected day at a selected time, repeat the deployment every day/week/month, and if defined, end on a specific date.

  In the Recurring page, you can set the following options for a recurring deployment:

  - ***When a device is refreshed:*** This option enables you to schedule a recurring distribution whenever the device is refreshed. In this option, you can choose to delay the next distribution until after a specific time.

    To set the delay, select the **Delay execution after refresh** check box, and specify the days, hours, and minutes of the time to delay the distribution.

    NOTE: The device is refreshed based on the settings in **Configuration** > **Device Management** menu > **Device Refresh and Removal Schedule** (Manual Refresh or Timed Refresh). Alternatively, you can refresh the device by selecting a device in the **Devices** page and clicking the **Refresh Device** option in the **Quick Tasks** menu.

  - ***Days of the week:*** This option enables you to schedule the distribution on selected days of the week.

    To set the day of distribution, select the **Days of the week** button, select the required day of the week, and set the start time of distribution. If you click the **More Options** link, additional distribution options appear. Click the **Hide Options** link to hide the additional distribution options and show only the default distribution options.

    - Selecting the **Use Coordinated Universal Time** check box enables you to schedule the distribution to all devices at the same time, regardless of time zone differences. Coordinated Universal Time (UTC), also known as World Time, Z Time, or Zulu Time, is a standardized measurement of time that is not dependent upon the local time zone. Deselecting UTC schedules the distribution at local time.

- Selecting the **Start at a random time between Start Time and End Times** check box activates the **End Time** panel in addition to the **Start Time** panel. You can specify the end time and the start time so that the distribution occurs at any random time between the start and end times.
- The **Restrict schedule execution to the following date range** option enables you to schedule a recurring distribution at the selected time, repeat the distribution on the days specified, and, if defined, end at the specific time. This option also enables you to restrict the distribution to the period between the start date and the end date. To set this option, select the **Restrict schedule execution to the following date range** check box and click the calendar icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

- ***Monthly:*** This option enables you to specify the monthly distribution options, where you can specify the following:
  - **Days of the month:** Enables you to schedule the distribution on a specific day of the month. You can specify any number between 1 and 31.
  - **Last day of the month:** Enables you to schedule the distribution on the last day of the month.
  - **Particular days of the month:** Enables you to schedule the distribution on specific days of every month. The valid options for the day are first, second, third, fourth, and fifth. The valid options for the weekday are Sunday through Saturday. To select one particular day of the month, use the drop-down arrows. An example is shown as follows.

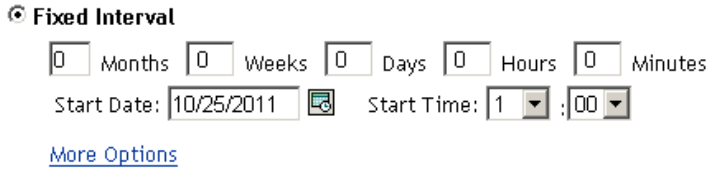
To select an additional day of the month, click the plus icon and use the drop-down arrows in the second row shown as follows:

NOTE: To remove a particular day from the list, click the minus icon.

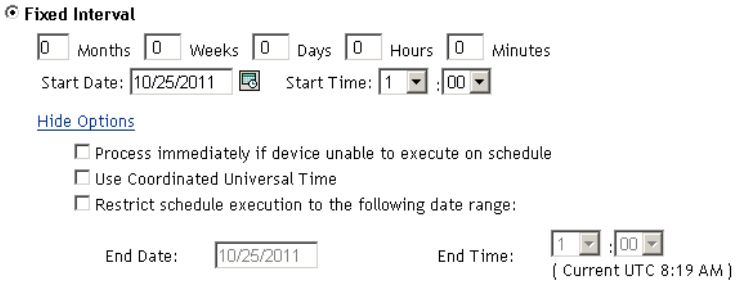
If you click the **More Options** link, additional distribution options appear. Clicking the **Hide Options link** hides the additional distribution options and shows only the default distribution options.

NOTE: The **Restrict schedule execution to the following date range** option enables you to schedule a recurring distribution at the selected time, repeat the distribution on the days specified, and, if defined, end on the specific time. This option also enables you to restrict the distribution to the period between the **Start Date** and the **End Date**. To set this option, select the **Restrict schedule execution to the following date range** check box and click the calendar icon to open the calendar and pick a start date or end date. Click the **Close** button when you have finished selecting the date.

- ***Fixed Interval:*** This option enables you to schedule a recurring distribution that runs after a fixed duration on a regular basis. You can choose the number of months, weeks, days, hours, and minutes of the interval and the start date for the distribution schedule.



If you click the **More Options** link, additional distribution options appear as shown in the following figure.



By default, the Device Refresh Schedule is set to twice a day. For testing and demonstration purposes, you could increase the frequency to once every five to fifteen minutes.

Notification and Reboot Options

In the Notification and Reboot Options page you can define whether users receive notification of patch deployments and reboots. You can also customize the notification. This page is only shown if you have selected the Custom remediation option in Step 5 of the wizard.

The page provides the following options:

- **Define Reboot Options:** Allows you to use the default reboot options you've set in options or override them and set them manually for the deployment.
  - ***Use values assigned to system variables or defaults:*** Uses reboot options set for deployments.
  - ***Override Settings:*** Overrides the default reboot settings and lets you choose from the options below.
- **Notify Users:** Select this option to notify the user prior to a reboot required for installation of the patch.
- **Description Text:** The text of the message that appears before patch installation completes and the computer reboots. You can edit this field only if you override the default settings.
- **Options:** When you define reboot options, you can specify whether to use the values in the default settings (the **Use values assigned to system variables or defaults** check box) or the custom settings. There are four options:
  - ***Suppress Reboot:*** If a patch requires a reboot by default, and no reboot is desired, select the **Suppress Reboot** option to stop this action. This will prevent a reboot after installation.
  - ***Allow User to cancel:*** On selecting this option, the user is allowed to cancel the reboot option.

- ***Allow User to snooze:*** On selecting this option, the user is allowed to snooze (pause) the reboot for a particular time.
  - **Snooze interval:** The amount of time before a user is prompted again to reboot after snoozing.
  - **Reboot within:** The amount of time before a user is forced to reboot for the deployment.
- ***Show tray notification:*** On selecting this option, a notification for a pending reboot is displayed in the system tray. If you select this option, define the following options
  - **Tray notification duration:** Option to select how long the system tray notification is displayed before being hidden.
  - **Tray notification text:** Option for text that appears in the notification.

  A a message prompt appears when a reboot is required.

  Depending on the notification settings configured, the prompt may include delay and cancellation options.

Click **Next** to define a deployment name.

Variables

The following is a list of the system variables which can be used through the console. These are the calls made to set the defaults. Each Variable has the variable name and the default setting. The values can be set by the user depending on their requirements.

- **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_REBOOT_TIMEOUT, “7200”);** Time to do prompts before rebooting, in seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_POPUP_SHOW_TRAY, "true");** Whether to show the popup in the corner.
- **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_POPUP_DURATION, "20");** How long to display the popup, in seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_MANDATORY_NOTIFY_REBOOT_SNOOZE_INTERVAL, "600");** The time to wait before showing popup again. In seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_REBOOT_TIMEOUT,"7200");**

  The time to wait before the system notifies a time out, in seconds.

- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_POPUP_SHOW_TRAY,"true");**
  The value indicates whether or not the system will show a popup before reboot.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_POPUP_DURATION,"20");**
  This value indicates the length of time for the popup to remain.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_REBOOT_SNOOZE_INTERVAL,"600");**
  The value sets the length of time for the snooze interval before reboot prompt, in seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_REBOOT_TIMEOUT,"7200");**
  The value shows the amount of time before the system reboots after an install timeout, in seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_POPUP_SHOW_TRAY,"true");**
  The value determines whether a popup appears to notify of install.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_POPUP_DURATION,"20");**
  This value sets the length of time that the popup will show for on install, in seconds.
- **ConfigManager.SetDefaultConfigValue(PATCH_NOTIFY_INSTALL_SNOOZE_INTERVAL,"600");**
  The value sets the length of time for the snooze interval after install, in seconds.

The following are no longer used:

- PATCH_NOTIFY_REBOOT_SNOOZE_TIMETOLIVE
- PATCH_NOTIFY_REBOOT_DIALOG_TIMEOUT
- PATCH_NOTIFY_INSTALL_SNOOZE_TIMETOLIVE
- PATCH_NOTIFY_INSTALL_DIALOG_TIMEOUT
- PATCH_MANDATORY_NOTIFY_ALLOW_SNOOZE
- PATCH_MANDATORY_NOTIFY_DIALOG_TIMEOUT
- PATCH_MANDATORY_NOTIFY_DIALOG_TIMEOUT_ENABLED
- PATCH_MANDATORY_NOTIFY_SNOOZE_HOURS
- PATCH_MANDATORY_NOTIFY_SNOOZE_MINUTES
- PATCH_MANDATORY_NOTIFY_SNOOZE_DAYS

Choose Deployment Name

The Choose Deployment Name of the Deploy Remediation Wizard lets you customize the name of the deployment you have scheduled.

The page provides the following options:

- **Deployment Name:** The name you give to the deployment.
- **Folder:** The location where the deployment is saved. The default location is `/Bundles/ZPM`.
- **Description:** A description of the scheduled deployment.

Deployment Summary

The Deployment Summary page displays a summary of the configuration made in the previous steps:

- **Deployment Name:** The name of the deployment as defined on the Choose Deployment Name page.
- **Delivery Schedule:** The schedule selected for distribution of patches as defined on the Distribution Schedule page.
- **Deployment Schedule:** The schedule selected for the deployments as defined on the Remediation Schedule page.
- **Total Selected Packages:** The total number of patches selected for deployment.
- **Order:** The order of deployment of the patches as defined on the Deployment Order and Behavior page.
- **Package Name:** The name of the patch you have selected for deployment.
- **Reboot:** The reboot setting of the selected patch as defined in the Deployment Order and Behavior page.

To complete the process of scheduling the deployment of a selected patch, click **Finish**. Click **Back** to return to the previous page. Click **Cancel** to exit the wizard.

Deploying Patches on Mac Devices

From ZENworks 23.3 onwards, the patch remediation on macOS devices is enhanced to support larger file patching without impacting the existing patching process.

After creating and deploying the remediation bundle, the newly introduced cURL feature kicks in to manage the larger file (only if the patch file size is more than 1 GB) patching. This feature provides a smoother remediation process for applying patches with large file sizes. The cURL provides resume-ability of patch downloading, which is required while downloading larger patch files. If the patch size is less than 1 GB, then the patch will be downloaded ondemand.

NOTE: Mac OS patching does not support Major OS Upgrade.

For example, using Mac OS patching, you cannot upgrade your macOS 12 device to macOS 13 or higher version.

Depending on the device platform (Intel or ARM), please refer to the following sections:

Applying Patches to Intel Devices

On Mac devices with Intel processors, perform the following steps to remediate patches:

1. In ZENworks Control Center, go to **Devices** > **Workstations**.
2. In the Workstations, select a macOS Intel device, and then click **Patches**.

   This page displays all the patches that are applicable to the device.
3. Select the required patch and click **Action** > **Deploy Remediation**.

4. In the subsequent screens, perform the required actions, and click **Next**.
5. In the Summary page, review the information, and then click **Finish**.

   The device will be patched using the remediation bundle.

Applying Patches to ARM Devices

On Mac devices with ARM/M1/ Silicon processors, perform the following steps to remediate patches:

1. On the macOS device, run `zac cru` (create-remediation-user).

   After running the command, enter the existing Volume User credentials. For more information, see Patch Management Commands in the ZENworks Command Line Utilities Reference.
2. After successfully running the command, in ZENworks Control Center, go to **Devices** > **Workstations**.
3. In the Workstations, select a macOS ARM/M1/ Silicon device, and then click **Patches**.

   This page displays all the patches that are applicable to the device.
4. Select the required patch and click **Action** > **Deploy Remediation**.
5. In the subsequent screens, perform the required actions, and click **Next**.
6. In the Summary page, review the information, and then click **Finish**.

   The device will be patched using the remediation bundle.

6 Best Practices

Depending on the state of patch updates, number and type of devices, and other variables in your management zone, you might initially have a significant number of patches being cached on the servers for distribution when you first apply patch policies. Patch policy implementation will incrementally reduce the patch workload over time. The information in this section will help you to make good decisions in both initial deployment of patch policies and managing them in the long term.

Below are a few general recommendations in regards to managing patches using ZENworks Patch Management:

1. Inventory the organization's IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization.
2. Monitor security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the software within the organization's inventory.
3. Prioritize the order in which the organization addresses remediating vulnerabilities.
4. Create patch policies in ZENworks Patch Management that are built on organizational priorities.
5. Conduct testing of patches and non-patch remediations on IT devices that use standardized configurations.
6. Oversee patch policy implementation.
7. Distribute vulnerability and remediation information to local administrators.
8. Perform automated deployment of patches to IT devices using patch policies.
9. Reconfigure automatic update of applications whenever possible and appropriate.
10. Verify vulnerability remediation through network and host vulnerability scanning.
11. Train administrators on how to apply vulnerability remediations using patch policies.
12. Verify that you have enough free disk space:
    - To initiate the patch scan, it is recommended that at least 500 MB of free disk space is available.
    - To deploy a Windows patch, it is recommended that the minimum disk space required is at least 5x the largest available patch. If you are deploying multiple patches, then the minimum disk space required is at least 5x the total size of the patches.

The ZENworks Server schedules a Vulnerability Detection task for all ZENworks managed devices (servers and workstations) and compiles information on the operating system, hardware, and software.

The results of the scan are sent to the ZENworks Server and can be viewed anytime in the Patches section in the **Patch Management** page or in the **Devices** page, even if a workstation is disconnected from your network.

- "Testing Patches" on page 86
- "Deploying Patches in a Controlled Way" on page 86

- "Monitoring Patch Implementation" on page 86
- "Tuning the Patch Management Service" on page 87

Testing Patches

Before you start downloading a patch, configure the downloading options in the **Configuration** page.

It is important that your organization determines a strategy for testing patches before release; this will vary from organization to organization, but should be in line with your current security policies. How you decide to test your patches before deployment will depend on your current architecture and policy. In some organizations it may be required to review your policies in order to effectively use this method.

However, it is highly recommended that patches are tested prior to deployment. For information on setting up test devices to implement patch policies, see Test a Policy Before Deploying to a Live Environment.

Deploying Patches in a Controlled Way

You can deploy patches using patch policies or Deploy Remediation. Since the integration of patch policies in ZENworks Patch Management, the manual process of Deploy Remediation, is generally used by exception. See Distribute and Apply Patches.

Patches are released frequently, and it is possible to automate the entire release process by using the deployment settings. While this may suit some smaller companies, in a large organization with multiple platforms and sites, we recommend that administrators design a strategy for deployment. Each patch for each software update will behave differently, which is why it is necessary to control the process. For example, some software will require a reboot after updating, and although ZENworks can manage this process on your behalf, your team should determine the details of this, and be aware of any other software or processes which are running, or patches that are being installed concurrently. The Best Practice recommendation for controlling these processes is to used a phased approach.

Implementing patch management tools in phases allows process and user communication issues to be addressed with a small group before deploying the patch application universally. Most organizations ?deploy patch management tools first to standardized desktop systems and single-platform server farms of similarly configured servers. Once this has been accomplished, organizations should address the more difficult issue of integrating multi-platform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations. Manual methods may need to be used for operating systems and applications not supported by automated patching tools, as well as some computers with unusual configurations; examples include embedded systems, industrial control systems, medical devices, and experimental systems. For such computers, there should be a written and implemented procedure for the manual patching process.

Monitoring Patch Implementation

Patch and vulnerability metrics fall into three categories: susceptibility to attack, mitigation response time, and cost, which includes a metric for the business impact of program failures. The emphasis on patch and vulnerability metrics being taken for a system or IT security program should reflect the

patch and vulnerability management maturity level. For example, attack susceptibility metrics such as the number of patches, vulnerabilities, and network services per system are generally more useful for a program with a low maturity level than a high maturity level. Organizations should document what metrics will be taken for each system and the details of each of those metrics. Realistic performance targets for each metric should be communicated to system owners and system security officers. Once these targets have been achieved, more ambitious targets can be set. It is important to carefully raise the bar on patch and vulnerability security to avoid overwhelming system security officers and system administrators.

Organizations should consistently measure the effectiveness of their patch and vulnerability management program and apply corrective actions as necessary.

For information on Patch Management monitoring tools, see the following:

- Security Pages
- Viewing Zone Patches
- Viewing Patches for a Device
- Accessing Patch Management Reports

Tuning the Patch Management Service

The following sections provide tuning information for the service:

- “Tuning the Patch Management Microservice” on page 87

Tuning the Patch Management Microservice

For modifying options related to JVM for the ZENworks Patch Management (ZPM) microservice patchsettings.sh should be modified.

This file is located at:

- On Linux: /etc/opt/microfocus/zenworks/settings

All the configuration files for the ZPM microservice are located under:

- On Windows: %ZENWORKS_HOME%/conf/patch-management
- On Linux: /etc/opt/microfocus/zenworks/patch-management

This primarily will have the following configuration files:

- application.properties: This file with all the needed configuration we have for the PLR processing and other important patch activities.
- batch.properties: This file consists of the configuration related to the spring batch.
- log4j2.xml: This file has all the logging-related configurations.
- patch-c3p0.properties: This file has the pooling configuration needed for the persistence.
- patch-ehcache.xml: This file has the caching configuration we use to improve the performance.
- patch-hibernate-configuration.properties: This file has the hibernate configuration we use in the microservice.

The following sections explain all the files in detail:

- "application.properties" on page 88
- "batch.properties" on page 89
- "log4j2.xml" on page 89
- "patch-hibernate-configuration.properties" on page 90
- "patch-ehcache.xml" on page 90
- "Prefetching of Patch Content" on page 91

application.properties

Metadata Processing Parameters

For the very first time, the agents send a lot of metadata, but once the metadata is processed, the number of operations is reduced. Even with a higher load, we recommend using the following default configurations:

```
# ThreadPoolExecutor configuration for metadata processing job
patch.metadata.batchjob.threadpool.maxPoolSize=1
patch.metadata.batchjob.threadpool.corePoolSize=1
patch.metadata.batchjob.threadpool.queueCapacity=20

# Poller configuration for metadata processing
poller.metadata.frequency=40000
poller.metadata.maxMessagesPerPoll=100
poller.metadata.wait.beforeRelease=100

# Max no. of signatures that should be inserted/updated in one job
max.metadata.per.iteration=5000
```

By default, keep only one thread to process metadata for all the PLR files, this helps in avoiding unnecessary locks and we do have a zookeeper lock mechanism at the Primary server level to avoid the database lock issues. If we need to slow down the metadata processing, we can reduce poller.metadata.maxMessagesPerPoll so that few files will be picked. Additionally, we can reduce the max metadata per iteration value to decrease processing speed. Increasing the poller.metadata.frequency will also help to increase the polling of the files in the patchlink folder under the collection directory.

NOTE: Do not increase both maxMessagePerPoll and frequency as it might not yield the optimum results. The above configuration in general would suffice.

Status Processing parameters

Once the metadata is processed, the PLR files will be moved to a status folder under patchlink for the further processing of patch & CVE statuses.

The following are the default configurations:

```
# ThreadPoolExecutor configuration for status processing job
patch.status.batchjob.threadpool.maxPoolSize=10
patch.status.batchjob.threadpool.corePoolSize=5
patch.status.batchjob.threadpool.queueCapacity=20
```

```
# Max no. of PLR files processed in 1 job execution
patch.status.batchjob.statefile.batchsize=10

# patch state file poller spec configuration
# frequency - fixed rate for PeriodicTrigger to poll for files
# maxMessagesPerPoll - max no. of messages(PLR files) to receive for each
poll.
# wait.beforeRelease - group timeout for aggregatorSpec

# Poller configuration for status processing
poller.status.frequency=60000
poller.status.maxMessagesPerPoll=100
poller.status.wait.beforeRelease=100
```

However, if the zone has less number of devices and you want to tune the settings accordingly by distributing the load. For example, for a zone with PostgreSQL with 5000 clients, the following configurations can be used:

```
patch.status.batchjob.threadpool.maxPoolSize=2   //only  two threads will
process status in parallel
patch.status.batchjob.threadpool.corePoolSize=1
patch.status.batchjob.threadpool.queueCapacity=4


patch.status.batchjob.statefile.batchsize=10


poller.status.frequency=90000   //Instead of polling for 1 min, we are
polling for every 1.5 minutes
poller.status.maxMessagesPerPoll=20 //For each poll we pick up 20 instead
of 100 files
poller.status.wait.beforeRelease=100
```

This configuration can process up to 20 files per 90000 ms (15 per minute), which effectively can process 900 PLR files for status in one hour, provided all the 20 files are processed before 90 seconds. This can be decreased or increased based on the distribution.

batch.properties

We don't recommend changing anything in this file. However, if we are increasing the maxPoolSize for the status in application properties, ensure to increase the below parameter proportionally.

```
batch.datasource.max-pool-size=25
```

The spring batch used in the PLR processing uses embedded h2 internally and if the threads increase for status processing, we observed that h2 connections also need to be incremented, or else the files will be skipped.

log4j2.xml

We use the following configuration in the log42.xml for the appenders' log level:

```
   <Properties>
       <Property name="LOG_PATTERN">[%-5p] [%d{yyyy-MM-dd HH:mm:ss}] [%t]
[%pid] [Patch-Management] [%T] [%c{1}] [%m]%n
       </Property>
       <Property name="APP_LOG_ROOT">${sys:zenworks.log.directory}/patch-
management</Property>
       <Property name="PATCH_LOG_LEVEL">DEBUG</Property>
       <Property name="HIBERNATE_LOG_LEVEL">WARN</Property>
       <Property name="SPRING_LOG_LEVEL">DEBUG</Property>
       <Property name="C3P0_LOG_LEVEL">WARN</Property>
       <Property name="TOMCAT_LOG_LEVEL">WARN</Property>
   </Properties>
```

Increase the log level only if needed, else setting the debug level will increase the verbosity and more logging. This will also impact the I/O and might lead to slow processing.

patch-hibernate-configuration.properties

This file has the configuration to override any hibernate configuration. It is not recommended to change the configuration unless you need to increase the processing by a large scale and even with higher processing requirements the default values are adequate.

patch-ehcache.xml

This file has the caching configuration and can be used to improve the performance.

The following are the configurations:

Cache names used during metadata processing:

- cvestatusps-cleanup-days-cache
- device-repository-cache
- cveid-within-ndays-cache
- all-patch-cve-details
- patch-signature-info-for-status-processing

Cache names used during status processing:

- patchlist-service-cache
- existing-patch-lastmodifed-info

Common use cases:

- zone-guid-cache //Used while fetching opaque data entries.
- patch-signature-repository-cache //Used for custom patches while deserializing PLR.
- system-setting-repository-cache //Used to cache system settings by name & object ID.
- custompatch-requirement-repository-cache //used in the construction of the DAU bundle.

Prefetching of Patch Content

Prefetching of content gives control over when the content gets downloaded from the web to the zone. During prefetch, the content gets downloaded to at least one of the OCM servers. The remediation of patches in agents will be relatively faster as agents need to download the content from Primary Servers and not from the web.

The customer can choose to precache the content in a few selected content servers. This way the content is available in content servers and remediation of patches will be faster than if we choose not to prefetch and not to precache the content. It is recommended to prefetch and precache the content for larger-size patches.

We have options on when to prefetch the content. The options are Manual **Pre-fetch Patch Content** action, Patch policy rebuild, and during Patch remediation deployment. It is recommended to prefetch the content during patch policy rebuild. This will speed up the content download part when the remediation of patches happens on the agent side.

It is recommended that you enable only the required languages which will consume disk space.

White-listing of external URL - https://forums.ivanti.com/s/article/URL-exception-list-for-Ivanti-Security-Controls?language=en_US

Managed Device

Setting a config value

On Managed devices, tuning parameters or configuring settings can be performed in different ways:

- Setting a system variable effective to a device. We can set it at the device level(overriding the zone level variable) or zone level.
- Creating the registry key on the device under HKLM/SOFTWARE/Novell/ZCM/ with key and value pair.

Scan

During scanning, we don't scan software installers by default as the number of patches will increase. Hence, they are excluded. However, if someone is interested in including the software installers for installing the application through ZENworks Patch Management, they can enable them by setting the following configuration value:

```
scan.software.installers - true
```

For metadata processing, we filter the superseded patches that are older than 2 years. However, this setting can be changed by tuning the following parameter:

```
superseded-years=2
```

The rest of the settings are best with the default configuration and no need to tune any other parameters.

Deployment

A patch can be deployed using the patch policy or a remediation bundle. During remediation, if we don't want certain patches to be installed, any of the following actions can be performed:

- Create a config key using system variable/registry with a key as ExcludedPatchesList and value with patch IDs separated by space ("ExcludedPatchesList", "patch1 patch2 patch3).
- Create a registry key under HKLM/SOFTWARE/Novell/ZCM/ExcludedPatches/ with patch ID as the key and value be any nonnull value.

It is recommended to spread the bundles (remediation/patch policy) so that the remediation will not be triggered parallelly. This reduces the cases where msiexec is waiting/failed because another instance is running. Hence, it is recommended to schedule the remediation instead of the remediating during the refresh and even in the schedule-based deployments, schedule the bundle to run in sequence than in parallel.

For reboot required patches, post remediation it is always recommended that the managed device is rebooted, as it can affect remediation of the subsequent patches.

Download

Content can be downloaded while scanning and performing the remediation. While scanning the patch catalog content is downloaded ondemand and while remediation the actual content is downloaded. The patch catalog is smaller in size approximately 20 MB where are patch content can be a huge file. Hence, it is recommended to distribute the content before performing the remediation. This can be performed by setting a distribution schedule against the patch policy/ remediation bundle. While downloading the content similar to the ZENworks Agent we need to handle the busy retries with incremental sleep. By default, we handle retries when the server returns 503(BUSY).

The following are the default settings:

```
max-busy-retries: 10 //max retries per server
max-sleep-between-retries: 2 //this will sleep for 2 seconds incremental
after all URLs are exhausted.
```

The default settings are sufficient to download content. If the server is busy and sending 503, then you can tune the above parameters.

Cleanup

The content under the ZPM directory will be cleaned if it is older than 7 days. For more aggressive cleanup, you can configure the cleanup using the following setting:

```
zpm-log-retain-days=7 //Content older than 7 days will be cleaned up.
```

Parameters can be tuned accordingly.

```
delete-results-folder=true //
```

By default, the results folder is not included in the cleanup for better debugging purposes. However, this can be overridden using the setting (not recommended).

7 Manage Patches

In the **Patches** page you can view and take actions on patches that display as a result of the DAU fingerprints that come from devices in the zone. These are manual actions you can do directly from the Patches page, or you can create patch policies in the **Patch Policies** page that do the patch actions automatically based on the schedules you define in patch policies and patch configuration. In ZENworks there is a Patches page to view the zone level patches and a Patches page to view the device level patches.

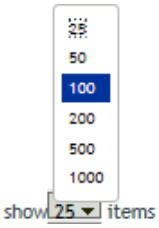
Manual actions in the Patches page include searching for patches, creating new patches from existing bundles, caching patches, and then deploying patches to managed devices. You can also do several house keeping functions to maintain the usefulness of the Patches page, including deleting, disabling, enabling, and even exporting patch entries. You can also refresh assignments using this page.

- "Configure the Patch Display" on page 93
- "View Patch Details" on page 94
- "Create a Custom Patch" on page 107
- "Delete a Patch" on page 109
- "Execute Action Menu Options" on page 111
- "Patch Details Page" on page 112
- "Patch Requirements" on page 116

Configure the Patch Display

This section explains features of the **Patches** page and how to use them.

To configure how many items show in the Patches panel, select a different item count in the drop-down menu at the bottom-right corner of the panel.



To sort patches alphanumerically, click on any column header in the table and it will sort based on that column. Clicking a header a second time reverses the order.

View Patch Details

Using the Patches page you can view the details of all patches that are applicable to the zone and you can also view information about all patches that are applicable for a specific device.

- "Zone-Level Patches" on page 94
- "Device Patches" on page 99

Zone-Level Patches

This page can be accessed by clicking the Security tab in the left navigation menu and then clicking the Patches tab. This page displays a list of all patches that are applicable to the zone and it provides the following information:

- "Patch Name" on page 94
- "Total Patches Available" on page 95
- "Patch Impact" on page 95
- "Patched" on page 96
- "Not Patched" on page 96
- "Patch Release Date" on page 97

Patch Name

The **Patch Name** is the name that identifies a patch. This name typically includes the vendor or manufacturer of the patch, the specific application, and version information.

An example of a patch name is shown as follows. It indicates that Adobe is the vendor, Adobe Flash Player is the application, and 21.0.0.242 is the version information:

Microsoft Patches:

- All Microsoft security patches are titled with their Microsoft Security Bulletin number in the format MS0x-yyy, where *0x* indicates the year the patch was released and *yyy* indicates the sequential number of the released patch. These patches are critical and must be installed as soon as possible.
- Names of all Microsoft non-security patches include the Knowledge Base (KB) article number. These patches can be installed at your discretion.
- The names of Microsoft service packs and third-party patches do not usually contain a KB number and never a Microsoft Security Bulletin number. Test these service packs thoroughly to ensure that they have the expected results.

For more information on the naming conventions for patches, refer to Comprehensive Patches and Exposures (CVE) (http://cve.mitre.org/), which is a list of standardized names for patches and other information exposures. Another useful resource is the National Patch Database (http://nvd.nist.gov/), which is the U.S. government repository of standards-based patch management data.

The patches shown in the Patches page have different icons indicating their current status. The following table describes the icons for each patch:

Patch Icon	Significance
	Indicates that the patch is disabled. Disabled patches are hidden by default. Use the **Include Disabled** filter in the **Search** panel to show these items.
	Indicates that only the fingerprint information for the patch has been brought down from the ZENworks Patch Subscription Network. This icon represents the patches that are neither cached nor pre-fetched.
	Indicates that a download or pre-fetch process for the patch bundles associated with the selected patch is pending.
	Indicates that a download or pre-fetch process for the patch bundles associated with the selected patch has started. This process caches or pre-fetches those patch bundles on your ZENworks Server.
	Indicates that the fingerprints and remediation patch bundles necessary to address the patch have been cached in the system. This icon represents the patches that are cached or pre-fetched and ready for deployment.
	Indicates that an error has occurred while trying to download or pre-fetch the patch bundle associated with the selected patch.
	Indicates that pre-fetching and caching is not applicable for the patch. This status is assigned to patches for which the ZENworks content system does not download and store the patch content. Instead, managed devices download the content directly from the patch vendor. Examples of these types of patches include vendor-channel delivered patches (SUSE, RHEL, Microsoft 365, Microsoft Office 2021) and macOS patches larger than 1GB in size.

Total Patches Available

The total number of patches that are available for deployment is displayed in the bottom-left corner of the Patches panel. In the following figure, the total number of available patches is 106:

Patch Impact

Each software vendor has their own way of classifying the level of need for an endpoint to have content deployed and installed. Vendors use labels such as **Critical**, **Important**, and **Moderate** to help describe how crucial their content is for securing the environment. But what if each vendor has a different definition of **Critical** or **Important?** It can be challenging to evaluate an environment's security posture accurately if you are relying on labels that vary from vendor to vendor.

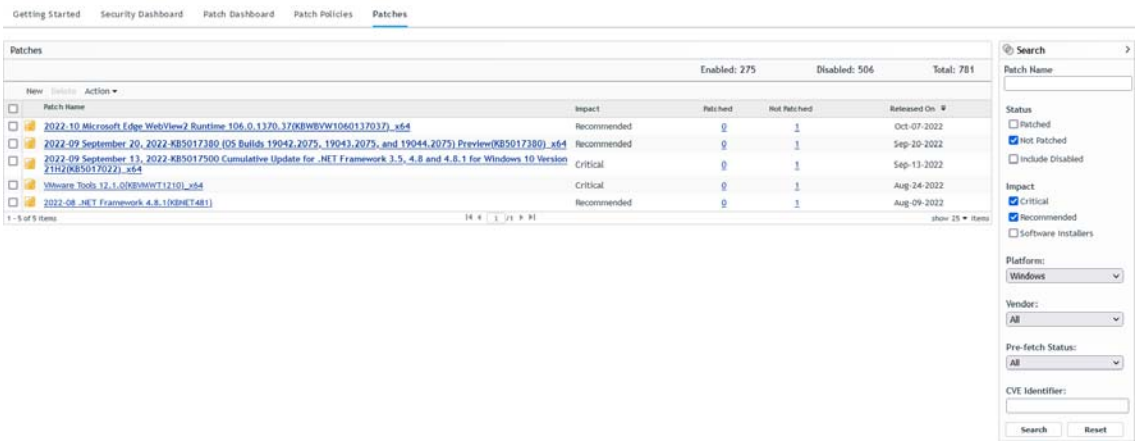
To address this confusion, ZENworks Patch Management replaces the vendor classification labels with our own. We call these labels content types and apply them to content from all vendors. Standardizing classification systems helps you to quickly identify the most crucial content needed to secure your endpoints, without having to look up each vendor's label individually.

For up-to-date information about our classification mappings, see the Patch Content Types and Mapping section in the ZENworks Patch Management Content Report.

Patched

The Patched column displays a link indicating the total number of devices to which the corresponding patch has been applied.

Click a link to display the Devices that are patched with the selected patch.



Not Patched

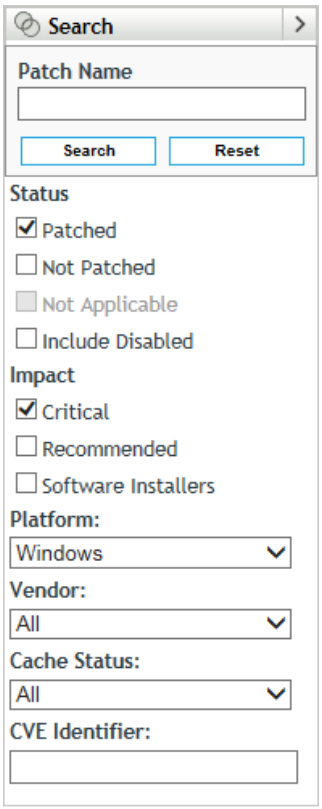
Displays a link indicating the total number of devices to which the corresponding patch has not been applied.Click a link to display the Devices on which the patch has not been applied as yet. You can deploy the patch to these devices by using the **Deploy Remediation** option.

Patch Release Date

The date the patch was released by the vendor is displayed in the right column under **Released On**. Click the **Released On** column to sort patches by their release date. All the patches released in the last 30 days are displayed in bold font.

Search Patches

The **Search** panel on the Patches page offers extensive search and data filtering options that allow you to search for specific patches and filter result sets based on the status and impact of the patches. Searching and filtering can be performed independently of each other or can be combined to provide extensive drill-down capabilities.



To search for a patch:

1. Type all or part of the patch name in the **Patch Name** text box.
2. Select applicable filter options; the CVE identifier must be typed.
3. Click **Search**.

To filter from all existing patches:

1. Leave the **Patch Name** text box empty.
2. Select applicable filter options.
3. Click **Search**.

NOTE: Click **Reset** to return to the default settings.

The following table describes the result of selecting each filter option under **Status**:

Status Filter	Result
Patched	Search results include all the patches in the patch list that have been applied to one or more devices.
Not Patched	Search results include all the patches in the patch list that have not been applied to any device.
Not Applicable	Search results include all the patches in the patch list that do not apply to the device.
Include Disabled	Search results include all the patches in the patch list that have been disabled by the administrator.

The following table describes the result of selecting each filter option under **Impact** (Impact Filters in Search):

Impact Filter	Result
Critical	Search results include all the patches in the patch list that are classified as Critical by ZENworks.
Recommended	Search results include all the patches in the patch list that are classified as Recommended by ZENworks.
Software Installers	Search results include all the patches in the patch list that are classified as Software Installers by ZENworks.

The following table describes the remaining filter options on the Search panel:

Filter	Result
Platform	Search results include all the patches relevant to the operating system in the patch list.
Vendor	Search results include all the patches relevant to the vendor in the patch list.
Cache Status	Search results include all the patches relevant to their cache status on the local server.
CVE Identifier	Search results include all the patches that have the common vulnerabilities and exposures ID that you type.
Relationships **NOTE:** This filter is only applicable to the Patches page on a selected patch policy.	Search results include patches for devices assigned to a patch policy, according to the option selected in the filter menu. For more information, see "Understanding the Relationships Filter" on page 99.

Understanding the Relationships Filter

The Search feature on the Patches page for a patch policy differs from the Search feature on the global Patches page by omitting the **Platform** filter and adding the **Relationships** filter. The Relationships filter enables you to limit and define the reporting of patch status according to the devices assigned to the patch policy as described below:

First 500 Devices

This is the default setting. It displays patch status for the first 500 devices assigned under the Relationships tab of a selected patch policy. If the policy is assigned to more than 500 devices, the complete list of devices can be viewed under Patched and Not Patched column values.

Test Devices

This option displays patch status for patches on designated test devices assigned to the selected patch policy.

Specific devices

Specific devices, device folders, or device groups will be listed under the Test devices option. For example, <computer name>, Workstations, Windows 10 Workstations and so forth can be assigned as a relationship to the patch policy.

When you filter on one of these relationship types, patch status will only be displayed for device patches that fall within that device criteria.

IMPORTANT: Due to the complexity of returning Patched and Not Patched results and the variables involved, a hundred percent accuracy for device counts in patch status is uncommon with large organizations. For example, if your organization has more than 500 devices assigned to a patch policy and you open the Patches page on that policy, the aggregate number of devices in the Patched and Not Patched columns is unlikely to reach 500 with the Relationships.

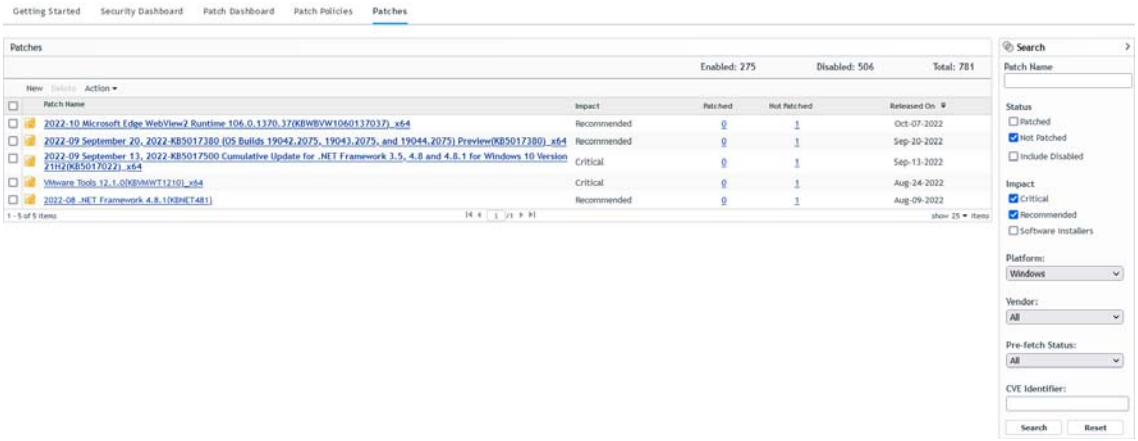
Device Patches

Using the Device Patches Page you can view information related to all patches, patch policies and remediation bundles assigned to the selected device. You can also perform actions for particular patches and refresh the assignments made to the device. The Device Patches page includes the following panels:

- “Patches” on page 100
- “Assigned Patch Policies” on page 104
- “Assigned Remediation Deployments” on page 104

Patches

Figure 7-1



This panel lists all the patches that are applicable to the device and provides the following information for each patch:

- "Patch Name" on page 100
- "Patch Impact" on page 101
- "Patched" on page 102
- "Assignments" on page 103
- "Release Date" on page 103
- "Installed On" on page 103
- "Installed By" on page 103

Patch Name

The **Patch Name** is the name that identifies a patch. This name typically includes the vendor or manufacturer of the patch, the specific application, and version information.

An example of a patch name is shown as follows. It indicates that Adobe is the vendor, Adobe Flash Player is the application, and 21.0.0.242 is the version information:

Microsoft Patches:

- All Microsoft security patches are titled with their Microsoft Security Bulletin number in the format MS0x-yyy, where *0x* indicates the year the patch was released and *yyy* indicates the sequential number of the released patch. These patches are critical and must be installed as soon as possible.

- Names of all Microsoft non-security patches include the Knowledge Base (KB) article number. These patches can be installed at your discretion.
- The names of Microsoft service packs and third-party patches do not usually contain a KB number and never a Microsoft Security Bulletin number. Test these service packs thoroughly to ensure that they have the expected results.

For more information on the naming conventions for patches, refer to Comprehensive Patches and Exposures (CVE) (http://cve.mitre.org/), which is a list of standardized names for patches and other information exposures. Another useful resource is the National Patch Database (http://nvd.nist.gov/), which is the U.S. government repository of standards-based patch management data.

When you click the patch name link, the Patch Details Page page is displayed.

Patch Impact

The **Impact** is the type of patch defined on the basis of the severity of the patch; the type can be Critical, Recommended, or Software Installers. Each impact is described as follows:

- **Critical:** ZENworks has determined that this type of patch is critical, and should be installed as soon as possible. Most of the recent security updates fall in this category.
- **Recommended:** ZENworks has determined that this patch, although not critical or security related, is useful and should be applied to maintain the health of your computers. You should install patches that fall into this category.
- **Software Installers:** These types of patches are software applications. Typically, this includes software installers. The patches show **Not Patched** if the application has not been installed on a machine.

Patch Management impact terminology for its patch subscription service closely follows the vendor impact terminology for patch criticality. Each operating system has a vendor-specific impact rating and that impact is mapped to a ZENworks rating as described in this section. Patch Management, following the recommendations of Lumension Security, increases or steps up the severity of the impact rating. For example, Microsoft classifications for Critical, Important, and Moderate patches are all classified as Critical by ZENworks.

The following table lists the mapping between ZENworks and Microsoft patch classification terminology:

Table 7-1 *ZENworks and Microsoft Patch Impact Mapping*

ZENworks Patch Impacts	Windows	Other
Critical	Critical Security	NA
	Important	
	Moderate	
Recommended	Recommended	NA
	Low	
	Example: Microsoft Outlook 2003 Junk E-mail Filter Update	
Software Installers	Software Distribution	Adobe 8.1 software installer
	Example: Microsoft Windows Malicious Software Removal Tool (Virus Removal)	

Patched

The Patched column indicates if the patch has been applied on the device or not. shows the relationship between a specific patch and the total number of devices (or groups) within ZENworks Server that meet a specific status. The patch statistics appear in two columns on the far right side of the Patches page. Each column status is described as follows:

The patches shown in the Patches page have different icons indicating their current status. The following table describes the icons for each patch:

Patch Icon	Significance
	Indicates that the patch is disabled. Disabled patches are hidden by default. Use the **Include Disabled** filter in the **Search** panel to show these items.
	Indicates that only the fingerprint information for the patch has been brought down from the ZENworks Patch Subscription Network. This icon represents the patches that are neither cached nor pre-fetched.
	Indicates that a download or pre-fetch process for the patch bundles associated with the selected patch is pending.
	Indicates that a download or pre-fetch process for the patch bundles associated with the selected patch has started. This process caches or pre-fetches those patch bundles on your ZENworks Server.
	Indicates that the fingerprints and remediation patch bundles necessary to address the patch have been cached in the system. This icon represents the patches that are cached or pre-fetched and ready for deployment.

Patch Icon	Significance
	Indicates that an error has occurred while trying to download or pre-fetch the patch bundle associated with the selected patch.
	Indicates that pre-fetching and caching is not applicable for the patch. This status is assigned to patches for which the ZENworks content system does not download and store the patch content. Instead, managed devices download the content directly from the patch vendor. Examples of these types of patches include vendor-channel delivered patches (SUSE, RHEL,Microsoft 365, Microsoft Office 2021) and macOS patches larger than 1GB in size.

NOTE: If you choose a patch that does not have cached remediation patch bundles, the deployment process might fail until the cache download is complete. You should download the files from the patch subscription and they must be packaged by ZENworks Configuration Management. Then the icon turns blue. To initiate an immediate download of these packages, select the Update Cache/ Patch Pre-fetch Content option from the Action menu.

Assignments

The name of the patch remediation bundle or policy assignment that includes the signature and is assigned to the device, is displayed in this column. When you click on the Assignment link, the Bundle or Policy Details page is displayed.

Release Date

The date the patch was released by the vendor is displayed in the right column under **Released On**. Click the **Released On** column to sort patches by their release date. All the patches released in the last 30 days are displayed in bold font.

Installed On

The date on which the patch signature was installed on the device, either through a remediation bundle, or through a patch policy. If the patch was not installed by ZENworks, this field will be empty.

Installed By

The name of the user who installed the patch on the device. If the patch was installed by ZENworks, then the value will be ZENworks. Else, if the patch was installed manually, for example, a Windows update, then the value will be Other.

The total number of patches that are available for deployment is displayed in the bottom-left corner of the Patches panel. In the following figure, the total number of available patches is 106:

NOTE: The total number of patches that are available for deployment is displayed in the bottom-left corner of the Patches panel.

Assigned Patch Policies

The Assigned Patch Policies panel displays all the enabled patch policies that are assigned to the device. This panel includes the following information:

- "Policy Name" on page 104
- "Version" on page 104
- "Enforcement Schedule" on page 104
- "Source" on page 104

Policy Name

The names of the enabled patch policies that are assigned to the device.

Version

The published version of the patch policy.

Enforcement Schedule

The schedule of when the policy is enforced on the device.

Source

Links to the source of the assignment, either the Device object's Summary page, the Device Group object's Summary page, or the Device Folder's Summary page. When you click the source, the object's Summary page is displayed. If there are multiple sources, they are displayed as an expandable hierarchy.

Assigned Remediation Deployments

This panel displays all the patch bundles that are assigned to the device. This panel includes the following information:

- "Deployment Name" on page 104
- "Folder" on page 104
- "Created On" on page 105
- "Enforcement Schedule" on page 105
- "Source" on page 105

Deployment Name

The remediation deployment name. When you click this link, the Bundle Summary page is displayed.

Folder

The path to the folder in which the bundle is saved.

Created On

The date on which the bundle assignment was created.

Enforcement Schedule

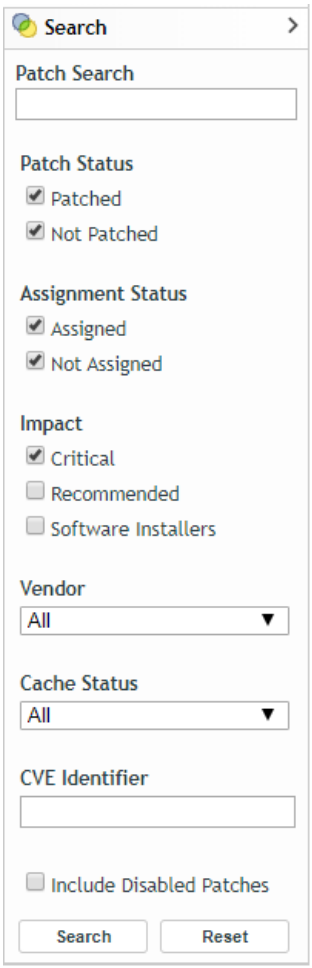
The schedule of when the deployment is enforced on the device. For example, Every Sun, Mon, Tue.

Source

Links to the source of the assignment, either the Device object's Summary page, the Device Group object's Summary page, or the Device Folder's Summary page. When you click the source, the object's Summary page is displayed. If there are multiple sources, they are displayed as an expandable hierarchy.

Search for Patches

The **Search** panel on the Patches page offers extensive search and data filtering options that allow you to search for specific patches and filter result sets based on the patch status, impact of the patches and assignment status. Searching and filtering can be performed independently of each other or can be combined to provide extensive drill-down capabilities.



To search for a patch:

1. Type all or part of the patch name in the **Patch Name** text box.
2. Select applicable filter options; the CVE identifier must be typed.
3. Click **Search**.

To filter from all existing patches:

1. Leave the **Patch Name** text box empty.
2. Select applicable filter options.
3. Click **Search**.

NOTE: Click **Reset** to return to the default settings.

The following table describes the result of selecting each filter option under **Status**:

Status Filter	Result
Patched	Search results include all the patches in the patch list that have been applied to one or more devices.
Not Patched	Search results include all the patches in the patch list that have not been applied to any device.
Not Applicable	Search results include all the patches in the patch list that do not apply to the device.
Include Disabled	Search results include all the patches in the patch list that have been disabled by the administrator.

The following table describes the result of selecting each filter option under **Assignment Status**.

Status Filter	Result
Assigned	Search results include all the patches in the patch list that have been assigned to one or more devices.
Not Assigned	Search results include all the patches in the patch list that have not been assigned to any device.

The following table describes the result of selecting each filter option under **Impact** (Impact Filters in Search):

Impact Filter	Result
Critical	Search results include all the patches in the patch list that are classified as Critical by ZENworks.
Recommended	Search results include all the patches in the patch list that are classified as Recommended by ZENworks.
Software Installers	Search results include all the patches in the patch list that are classified as Software Installers by ZENworks.

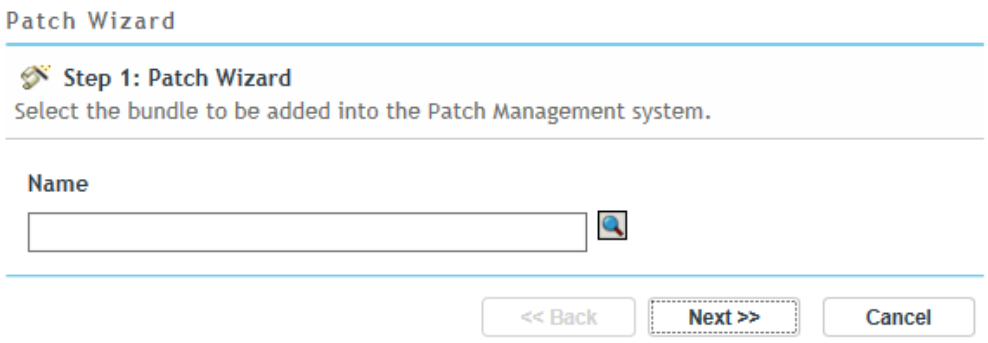
The following table describes the remaining filter options on the Search panel:

Filter	Result
Platform	Search results include all the patches relevant to the operating system in the patch list.
Vendor	Search results include all the patches relevant to the vendor in the patch list.
Cache Status	Search results include all the patches relevant to their cache status on the local server.
CVE Identifier	Search results include all the patches that have the common vulnerabilities and exposures ID that you type.
Relationships **NOTE:** This filter is only applicable to the Patches page on a selected patch policy.	Search results include patches for devices assigned to a patch policy, according to the option selected in the filter menu. For more information, see "Understanding the Relationships Filter" on page 99.

Create a Custom Patch

The Patch Wizard assists in selecting existing patch bundles and modifying patch details to create a custom patch. If you are not using an existing bundle, you will need to create a bundle of the patch contents before creating a customized patch. For more information, see "Creating Bundles" in the *ZENworks Software Distribution Reference*.

When you select the New menu item on the Patches page or Recently Released Patches panel, the Patch Wizard appears as shown below:



To create a customized patch:

1. Click the New menu item on the Patches page to open Step 1 of the Patch Wizard.
2. Click the Browse icon and navigate to the desired bundle in the Browse for Folder dialog box.
3. After selecting the desired bundle, click OK to confirm the bundle selection and then click Next.

NOTE: You can associate only one bundle with a patch.

4 Click **Next** to advance the Wizard to Step 2 to where you can add or modify details about the patch. Any of the fields can be modified.

5 In the Define Patch Details screen, add or modify details about the patch and then click **Next**. *Any of the fields can be modified*. The fields include:

Item	Definition
Name	The name of the patch.
Impact	The impact of the patch as determined by ZENworks.
Vendor	The name of the vendor.
Vendor Product ID	The ID number given to the product by the vendor.
Release Date	The date on which the patch was released.
Size	The size of the patch bundle.
Description	The description of the patch; includes detailed information concerning the defect or issue resolved by this patch, deployment notes, and the prerequisites for deployment.
URL	The URL of the Vendor's website, which includes additional information about the patch.
Requires Reboot	Whether a reboot is required after patch deployment.

6 In the Define Applicability Requirements screen, specify the requirements that must be met for the patch to be applicable on a device. You need to define requirements through the use of filters. A filter is a condition that must be met by a device in order for the patch to be applied. For example, you can add a filter to specify that the device must have exactly 512 MB of RAM in order for the patch to be applied, and you can add another filter to specify that the hard drive be at least 20 GB in size. Specify the applicability requirement filters and click **Next**.

NOTE: For information about Filters, see Filter Conditions and Filter Logic in the ZENworks Software Distribution Reference.

7 In the Define Patched Requirements page, specify the requirements that must be met for the device status to be changed from Not Patched to Patched and then click **Next**. By default, when a patch bundle is installed successfully, the status is displayed as Patched.You can change the requirement or add additional requirements.

8 The Summary page of the Patch Wizard displays the summary of the details of the patch you have created in the previous steps. Summarizing the important details of the patch is the last step in creating a custom patch. The details include the following information:

- Patch Name: The name of the patch.
- Bundle: The name of the bundle that is included in the patch.
- Impact: The impact of the patch as determined by ZENworks. See Patch Impacts.
- Vendor: The name of the vendor or manufacturer of the patch.

- Vendor Product ID: The ID number given to the product by the vendor.
- Release Date: The date on which the patch was released.
- Size (KB): The size of the patch bundle.
- Description: The description of the patch; includes detailed information concerning the defect or issue resolved by this patch, deployment notes, and the prerequisites for deployment.
- URL: The URL of the Vendor's website that includes additional information about the patch.
- Requires Reboot: Indicates whether the device needs to be rebooted or not after the patch is applied.
- Applicability Requirements: Click the Back button to view the Applicability Requirements page and review or edit the defined requirements.
- Patched Requirements: Click the Back button to view the Patched Requirements page and review or edit the defined requirements.
- Run the Patch Server maintenance update to add the Custom Patch to the DAU bundle: Select this option to include the custom patch bundle in the DAU bundle and scan for applicable devices.
- Define additional details: Select this option to define additional details for the patch.After the patch is created the Patch Details page is displayed, enabling you to make the required changes.

Click **Finish** to complete the process of creating a custom patch.

NOTE: After creating a new patch, you cannot immediately deploy it to the applicable devices. A Patch Server maintenance update is required to complete after the custom patch is created in ZENworks Control Center. After the update, a new Discover Applicable Updates (DAU) bundle version is created with the custom patch information. Applicability of the new custom patches to the managed devices will be based on their bundle system requirements evaluation after the DAU bundle is successfully applied and patch scan is completed.

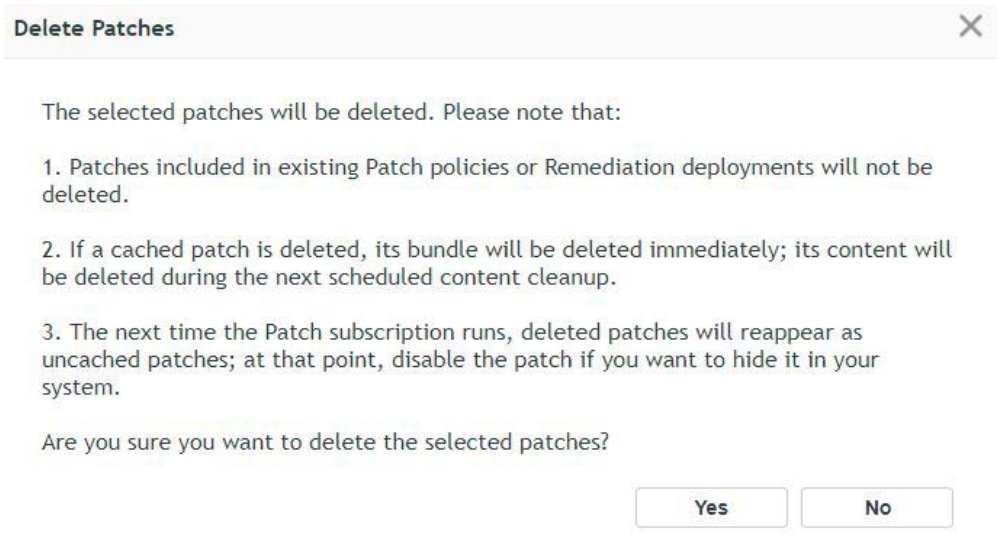
Delete a Patch

The Patches section enables you to remove patches from the Patch Management System.

To delete a patch:

1 Select the check boxes for the patches you want to delete, and click the **Delete** menu item.

A message appears, asking you to confirm patch deletion.



2 Click **Yes** to confirm the deletion. Click **No** to return to the Patches page.

When you select Yes:

- The patches included in the existing Patch policies or Remediation deployments will not be deleted.
- If a cached patch is deleted, its bundle will be deleted immediately. However, its content will be deleted only during the next scheduled content cleanup.
- The next time the Patch Service update is run, the deleted patches will reappear as uncached patches. At that point, disable the patch if you want to hide it in your system. To cache the patches the user will have to either manually cache them or include them in a Patch policy.

IMPORTANT: If any of the patches you are deleting are deployed, those patches and their associated bundles are not deleted. In this case, when you click **Yes** to the Delete Patches message, another prompt will open, informing you of the dependencies to deployed bundles and their bundle identification numbers. These bundles can be from patch policies and/or patch remediations.

Any indicated dependencies must be resolved before the patches associated to them can be deleted. The services-messages log shows the patches that cannot be automatically or manually deleted because of dependencies. The location of the log is provided below:

- Linux: `var/opt/microfocus/log/zenworks/ZENworksClientMgmt/services-messages.log`

Execute Action Menu Options

From the **Action** menu you can perform one of five actions to patches that are selected in the Patches page. Descriptions of these actions are provided below:

- **Deploy Remediation:** To use this option, select the check boxes for the patches you want to deploy and select **Deploy Remediation** from the **Action** menu options to open the Deploy Remediation Wizard. For more information, see Deploying Patches Manually.
- **Enable:** After selecting one or more disabled patches, click this option to enable them. Disabled patches will only display in the Patches page if the **Include Disabled** check box is selected when a search is executed.
- **Disable:** After selecting one or more patches, click this option to disable them. The selected patch is removed from the list and will only be displayed when the **Include Disabled** check box is selected during a completed search.

  Disabling a patch also disables all the bundles associated with it.
- **Pre-fetch Patch Content:** Initiates the patch pre-fetch process for the bundles associated with the selected patch and pre-fetches those bundles on your ZENworks Server.

  The remediation patch bundles must be cached before they are installed on the target device.

  To use this option:

  1. Select one or more patches in the patches list.
  2. In the Action menu, click Pre-fetch Patch Content.

  The patch icon changes color to indicate process initiation. When the pre-fetch is in progress, the icon changes to white . When pre-fetch is complete, the color of the patch icon changes to green . This indicates that the patch remediation is ready to be deployed.
- **Export:** Details such as the status and impact of all patches can be exported into a comma-separated value (CSV) file. You can choose to save the file in a different file format after opening it from the download option.

  To use this option, select the patches you want to export and click **Export** in the **Action** drop-down menu.

  The result and follow-on steps after clicking **Export** will vary depending on your browser and browser settings. The file may download immediately to your local download folder, or the browser may present you with an option to open or to save the file.
- **Create Patch Tracker Dashlet:** Enables you to create a Patch Tracker dashlet from the selected patches. For more information, see "Patch Tracker Dashlet" on page 45.

  NOTE: The Patch Tracker dashlet cannot be created from the disabled patches.

NOTE: To know when a patch is downloaded, view the **Message Log** panel for that patch in the **Bundles** section.

Patch Details Page

When you select a particular patch, all information related to the selected patch is displayed. The Patch details are displayed in three tabs, they include the following:

- “Patch Information” on page 112
- “Relationships” on page 115
- “Devices” on page 116

Patch Information

The Patch Information tab is displayed by default when you click the Patch name link in the Security Dashlets page, Patches page (patches applicable for the entire zone) or the Patches page (patches applicable for a particular device). This page displays the following information:

Patch Status

Indicates if the patch is enabled or disabled. If the patch is disabled, the reason for the patch being disabled, along with the date on which it was disabled, is displayed.

Impact

Indicates the impact level of the patch. The impact levels include Critical, Recommended, or Software Installers. For more information, see “Patch Impact” on page 95.

Download Status

Indicates the status of the patch download. Based on the Patch server configuration, the patches are downloaded from the patch repository to a particular server. The status of the download is indicated in this column. The values include:

- : Indicates that the fingerprints and remediation patch bundles necessary to address the patch have been cached in the system. This icon represents the patches that are cached or pre-fetched and ready for deployment.
- : Indicates that only the fingerprint information for the patch has been brought down from the ZENworks Patch Subscription Network. This icon represents the patches that are neither cached nor pre-fetched.
- : Indicates that a download or pre-fetch process for the patch bundles associated with the selected patch is pending..
- : Indicates that a download or pre-fetch process for the patch bundles associated with the selected patch has started. This process caches or pre-fetches those patch bundles on your ZENworks Server
- : Indicates that an error has occurred while trying to download or pre-fetch the patch bundle associated with the selected patch.

- : Indicates that the patch is disabled. Patches that are superseded by newer patches are automatically disabled.

  Disabled patches are hidden by default. Use the Include Disabled filter in the Search panel to show these items.

- : Indicates that pre-fetching and caching is not applicable for the patch. This status is assigned to patches for which the ZENworks content system does not download and store the patch content. Instead, managed devices download the content directly from the patch vendor. Examples of these types of patches include vendor-channel delivered patches (SUSE, RHEL, Microsoft 365, Microsoft Office 2021) and macOS patches larger than 1GB in size.

NOTE: If you choose a patch that does not have cached remediation patch bundles, the deployment process might fail until the cache download is complete. You should download the files from the patch subscription and they must be packaged by ZENworks Configuration Management. Then the icon turns blue. To initiate an immediate download of these packages, select the Update Cache/ Patch Pre-fetch Content option from the Action menu.

Vendor

Indicates the name of the vendor who has published the patch.

Vendor Product ID

Indicates the Product ID of the vendor who has published the patch.

Release Date

Indicates the date on which the patch was published for public access.

Size

Indicates the size of the patch file.

Description

Displays a description of the patch as provided by the Vendor. The description of the patch includes detailed information concerning the defect or issue resolved by this patch, deployment notes, and the prerequisites for deployment. To view the entire information, click the Show More link that is displayed against the Description.

URL

The URL to the Vendor’s website which provides detailed information about the patch. As a best practice, it is recommended that you visit the URL to identify if there are any patches that are required to be applied before applying the selected patch. Especially for Microsoft patches.

Installation Details

Indicates if the system needs to be rebooted after the patch is installed and also indicates if the patch can be uninstalled when required.

CVEs Addressed by Patch

Lists the Common Vulnerabilities and Exposures (CVEs) that are addressed by the patch. The CVE details include the CVE ID and a summary of the CVE. Clicking the CVE ID will display the CVE details page. For information on the CVE page, see the CVE Information Page in the *CVE Reference*.

When you enable the Include CVEs inherited from superseded patches filter, CVEs, that are directly associated with the patch and CVEs that are inherited through the superseded patches are displayed. However, if you disable this filter, only CVEs that are directly associated with the patch are displayed. By default, this filter is disabled. When you click a CVE, the page is displayed.

NOTE: For Custom Patches, you can click the **Add/Remove** link to add or delete CVEs addressed by the patch.

Supersedence Details

This section of the page provides information about the patches that supersede the selected patch and information about the patches that have been superseded by this patch:

- Superseded By: Lists the patches that supersede the selected patch. Clicking a patch link will display the Patch Information page for the selected patch.
- Supersedes: Lists the patches that are superseded by the selected patch. Clicking a patch link will display the Patch Information page for the selected patch.

Disabled Patches

The disabled patches are indicated by . Patches that are superseded by newer patches are automatically disabled. Disabled patches are hidden by default. Use the Include Disabled filter in the Search panel to show these items.

To enable patches, perform the following steps:

1. In the Patches page, use the Include Disabled filter in the Search panel to view the disabled patches.
2. Select the disabled patch, click Action, and then select Enable.

IMPORTANT: After enabling the patch, ensure that you rerun the patch scan on all the managed devices where the selected patches are applied.

The patches that were enabled will remain enabled until they are manually disabled.

When you deploy remediation for the newly enabled patch, only the latest available version is installed. However, the earlier versions will be marked as installed.

Relationships

This page provides information about the patch policies and the remediation bundles that have been created for the selected patch. This page includes the following details:

Patch Policies

This panel lists all the policies associated with the selected patch and provides the following information:

- Policy Name: The name of the patch policy. When you click the link, the Summary page of the Patch Policy is displayed.
- Bundle Folder: The Bundle folder that contains the policy's bundle. When you click this link the Bundles folder page is displayed.
- Enabled: Indicates if the patch policy is enabled or not.
- Version: Displays the published version of the patch policy.
- Has Sandbox: Indicates if the patch policy has a sandbox version or not.

Remediation Deployments

This panel lists all the remediation deployments associated with the selected patch and provides the following information:

- Deployment Name: The name of the remediation deployment associated with the patch. When you click this link the Deployment bundle's Summary page is displayed.
- Bundle Folder: The location of the bundle folder for the patch remediation deployment. When you click the link, the bundle folder that contains the deployment bundle is displayed.
- Enabled: Indicates if the remediation deployment is enabled or not.
- Version: Displays the published version of the remediation deployment bundle.
- Has Sandbox: Indicates if the remediation deployment bundle has a sandbox version or not.

Patch Bundles

This panel lists all the patch bundles associated with the selected patch and provides the following information:

- Bundle Name: The name of the patch bundle that is associated with the patch.
- Bundle Folder: The location of the bundle folder that includes the patch. When you click the link, the bundle folder is displayed.
- Enabled: Indicates if the patch bundle is enabled or not.
- Version: Displays the published version of the patch bundle.
- Has Sandbox: Indicates if the patch bundle has a sandbox version or not.

Devices

This tab provides information about the various devices that are impacted by the selected Patch. This tab displays the following information:

- Name: The name of the device that is impacted by the selected patch. When you click this link, the device summary page is displayed.
- Operating System: Displays the operating system of the selected device.
- Last Patch Scan: Displays the date on which the last patch scan was performed on the device.
- Patched: Indicates if the patch has been applied on the device or not.
- Assignments: Lists the number of assignments for the patch that have been made to the device. When you click the count, the details of the assignments are displayed.
- Installed On: Displays the date on which the patch was installed on the device.
- Installed By: Indicates if the patch was installed on the device by ZENworks or it was installed manually (through other sources).

Patch Requirements

This page enables you to edit the Applicability Requirements and the Patched Requirements that are defined for a Custom Patch while creating the patch using the Custom Patch wizard. Administrators need to have Patch Configure, Bundle View and Bundle Author rights to successfully view and change the Applicability Requirements and the Patched Requirements. This page includes the following panes:

- "Applicability Requirements" on page 116
- "Patched Requirements" on page 116

Applicability Requirements

This pane provides information about the filters that are defined as Applicability Requirements for a Custom Patch. If no requirements were specified during the creation of the custom patch, you can define them using this page. The patch bundle is considered applicable to devices based on the selected filters. You can add, edit or delete filters in this section.When you make any edits to the Applicability Requirements, the bundle version is incremented.

Patched Requirements

This pane provides information about the filters that were defined as Patched Requirements for a Custom Patch. Devices are considered patched based on the selected filters. You can add, edit or delete filters in this section.

A Troubleshooting

This troubleshooting appendix is intended to help you resolve issues when managing Patch Management. It contains error codes and issues you might encounter, as well as many of the actions you can take to resolve these issues.

Many issues can be avoided by following the guidance in the Patch Policy - Best Practices section in this reference. If you have not already evaluated your Patch Policy configuration with this guidance, we recommend that you do so.

For information about system variables that you can use in Patch Management to enable or disable patch related features, see Appendix B, “System Variables,” on page 135.

In many cases patch issues that occur are not related to the Patch Management software or configuration, but can be a problem with a patch itself or an environment issue. Before referring to the content in this appendix, you may want to review the actions below to see if they can help resolve your issue:

- Read event logs to see if there is any indication of native hardware, software, or environment issues that need to be resolved.

  The *WSH* types will show the actions taken by ZPM to apply the patch. *Msiexec* or other errors may also be seen.
- Determine if the target device meets patch requirements, such as operating system, Bit-level, and so forth.
- Execute a search for error codes to determine if the issue is vendor or Patch Management related.
- Apply the patch using the vendor's patching mechanism.

  For example, if it is a Microsoft Windows update, use Windows Update to apply the patch. If it fails repeatedly AND fails on multiple machines, the patch is probably bad and needs to be fixed by the vendor. You should contact the vendor directly to report the issue.

More troubleshooting information is provided in the sections below:

- “Patch Management Issues” on page 117
- “Configuration Issues” on page 124
- “Error Codes” on page 125

Patch Management Issues

This section contains detailed explanations of the error messages you might receive or problems you might encounter when using ZENworks Patch Management. You can also reference these online references:

- Knowledgebase

- Technical Support Handbook
- Cool Solutions

NOTE: If you cannot resolve an issue related to Patch Management using this troubleshooting section or the online resources above, please contact Technical Support.

Review the issues below to see if any them are applicable to your patch environment and take the prescribed action where needed.

- “Patch Pre-fetch Fails while Rebuilding Policies” on page 119
- “Patch Content Download Fails for the Slack Software” on page 119
- “Unable to Trigger Patch Scan on SLES Devices” on page 119
- “The Version Installed with the Remediation Bundle and Version Available on The Device Are Not Identical” on page 120
- “The Patch Scan Fails on Linux Agents” on page 120
- “Superseded Patch Updates are not Pre-cached in the Airgap Server” on page 120
- “Patch settings are hidden even after activating the Patch Management license” on page 120
- “In the Advanced Patch Feed, the Patch Deployment with Reboot Action Fails” on page 121
- “Patches are unavailable because of connectivity or firewall issues” on page 121
- “Unable to Select Primary Server as Patch Server After Migrating to The New Patch Feed” on page 121
- “No patches are shown in the Patches page” on page 121
- “Patch remediation bundles are not replicating to Primary servers” on page 122
- “Patches do not seem to be deployed on the target device” on page 122
- “The Cancel button disappears in the Reboot Required dialog box” on page 122
- “Superseded patches are shown as NOT APPLICABLE” on page 122
- “Patch deployment might not start when scheduled” on page 123
- “Linux - Custom Patches: Bundles fail to launch” on page 123
- “Airgap Server: User receives trial license email after adding the license info to system variables” on page 123
- “Blank PowerShell window is displayed after deploying patch policies during device shutdown” on page 123
- “Unable to uninstall patches” on page 124
- “Patch Policy assignment: Bundle stays in ‘Pending’ state forever” on page 124
- ““Remediation cannot be deployed” error is displayed when remediating vulnerable devices from security dashboard” on page 124

Patch Pre-fetch Fails while Rebuilding Policies

Source: Patch Management

Explanation and Possible Cause:When you assign a patch policy to devices, and when the patch policy gets rebuilt either manually or as part of the rebuild schedule, all the patch IDs that are part of the rebuild process get added to the pre-fetched list. If the number of assigned devices is more than 1000, then the patch pre-fetch fails while rebuilding policies.

For more information on pre-fetching of patches, see Understanding Pre-Fetching and Pre-Caching of Patches.

Action: After assigning the patch policies, ensure that you perform assignment recomputation to prefetch the data.

To perform assignment recomputation, perform any one of the following instructions:

- Run the precomputation by using the zman area command.

  For more information, see Assignment Commands in ZENworks Command Line Utilities Reference.
- Configure Assignment Optimization Settings in ZCC.

  To configure the optimization settings, in ZCC, go to Configuration > Management Zone Settings > Infrastructure Management > Assignment Optimization Settings.
- Go to the Device Assignment Status dashboard and perform a refresh for assignment recomputation.

Patch Content Download Fails for the Slack Software

Source: Patch Management, Advanced Patch Feed

Explanation: In the Advanced Patch Feed, when you try to perform the remediation of the Slack Software, the patch content download fails.

Action: Install the patch using Custom Patch. For more information, see Create a Custom Patch.

Unable to Trigger Patch Scan on SLES Devices

Source: ZENworks 23.3, Patch Management

Explanation: Patch Scan might not be triggered on SLES devices.

Possible Cause: This might be due to missing RPMs. Ensure that the following RPMs are available on the device:

- libicu65_1-ledata-65.1-150200.4.5.1.noarch
- libicu-suse65_1-65.1-150200.4.5.1.x86_64

Action: Run the following command to install the missing RPMs:

```
rpm -ivh <rpmname>
```

In the above command, replace “rpmname” with the following RPMs:

- libicu65_1-ledata-65.1-150200.4.5.1.noarch
- libicu-suse65_1-65.1-150200.4.5.1.x86_64

The Version Installed with the Remediation Bundle and Version Available on The Device Are Not Identical

Source: ZENworks 23.3, Patch Management, Advanced Patch Feed

Explanation: A browser version installed with Remediation Bundle and the browser version available on the device is not identical.

Possible Cause: When Auto-update for a browser is enabled, then the version installed using Remediation Bundle might be updated to the latest available version. Hence, the version installed using the remediation Bundle and the version available on the device might not be identical.

Action: Disable the auto-update feature on the browser.

The Patch Scan Fails on Linux Agents

Source: ZENworks 23.3, Patch Management, Advanced Patch Feed

Explanation: In the Advanced Patch Feed, the patch scan fails on Linux (SLES 12 and SLED 12) agents, and the Error while initializing scanner message is logged in the PatchScan log file.

Action: Patch Management does not support SLES12 SP4 and below versions. Ensure that you update the device to a higher SLES version that is supported by Patch Management.

Superseded Patch Updates are not Pre-cached in the Airgap Server

Source: ZENworks 23.3, Patch Management, Advanced Patch Feed

Explanation: In the Airgap zone, superseded patch updates are not pre-cached

Possible Cause: This might be due to the behavior that the superseded patch might not be detected during the first scan and thereby the patch will not be pre-cached.

Action: The issue will be resolved during the next transfer of patch content to the Airgapped (importer) zone.

Patch settings are hidden even after activating the Patch Management license

Source: ZENworks; Patch Management

Explanation: Some of the patch-related settings are hidden even after successfully activating the Patch Management license.

Possible Cause: This might happen only when the administrator deactivates Patch Management and then reactivates Patch Management in the evaluation mode or by providing a key.

Action: After activating the license, log out and re-login to ZCC.

In the Advanced Patch Feed, the Patch Deployment with Reboot Action Fails

Source: Advanced Patch Feed, ZENworks 2020 Update 3, Patch Management

Explanation: In the Advanced Patch Feed, when you initiate a patch scan on older agents and deploy a patch with reboot action, the patch deployment and patch reboot might not work as expected.

Action: None.

Patches are unavailable because of connectivity or firewall issues

Source: ZENworks; Patch Management.

Explanation: Ensure that your server environment can access patch providers and hosts and that applicable clients are properly configured for Office 365 updates.

- **Post Patch Management migration:** If you have migrated Patch Management to the Advanced Patch Platform, the partner URLs listed in the document referenced below must be allowed access in the Firewall policies to enable the Patch Service to download patch content for other vendors such as Microsoft and Adobe.

  https://www.microfocus.com/documentation/zenworks-resources/ZPM_URLs.xlsx

- **Pre-Patch Management migration:** If you have not yet migrated Patch Management and are still using the Legacy Patch Platform, see this same section in the *ZENworks 2020 Update 2 Patch Management Reference*:

  "Patches are unavailable because of connectivity or firewall issues"

Unable to Select Primary Server as Patch Server After Migrating to The New Patch Feed

Source: Patch Management

Explanation: After migrating to the new patch feed, when you try to assign a Primary Server as a Patch Server, an Unable to connect to Patch Service error message is displayed.

Action: Check if the patch service is running. If the patch service is running, then if you had configured a proxy- server before migrating to the new patch feed, then ensure that you reconfigure the proxy server again (System Update Entitlement Proxy Server should be configured. In ZCC go to Configuration > Management Zone Settings > System Update Settings > Proxy server settings).

No patches are shown in the Patches page

Source: ZENworks; Patch Management.

Possible Cause: The server has just been installed.

Action: You need to wait for managed devices to run a patch scan and report their results. Patches will begin to appear at that time.

Patch remediation bundles are not replicating to Primary servers

Source: ZENworks; Patch Management.

Possible Cause: The patch remediation bundle(s) was modified.

Action: Patch remediation bundles from patch policies or deployment remediations should not be modified.

Patches do not seem to be deployed on the target device

Source: ZENworks; Patch Management.

Possible Cause: The ZENworks administrator has not deployed the patches into the applicable devices in the ZENworks server, or the patches have been deployed in the server but the device refresh schedule has not been triggered in the ZENworks Agent.

Actions: Check to see if the **Device Refresh Schedule** option is set as **Manual Refresh** or **Timed Refresh** on the Configuration page, and wait for the specified interval.

The Cancel button disappears in the Reboot Required dialog box

Source: ZENworks; Patch Management.

Explanation: When two or more patches are deployed, if the **Allow User to Cancel** option is set as No on the Pre Install Notification Options page and the Notification and Reboot Options page of the server, the **Cancel** button disappears in the Reboot Required dialog box for all patches of the agent.

Action: None necessary.

Superseded patches are shown as NOT APPLICABLE

Source: ZENworks; Patch Management.

Explanation: In earlier releases of Patch Management, a patch showed its status as PATCHED or NOT PATCHED, regardless of whether the patch was new or outdated. This often caused many more patches to show as NOT PATCHED than were actually necessary for deployment to a given target device. This issue has been addressed in many of the new advanced content patches provided with ZENworks 2017:

- When a patch is superseded, it is automatically disabled.
- If the patch is re-enabled and detected, in most cases the patch shows as NOT APPLICABLE because it has been replaced by a superseded patch. However, if the device has not installed the superseding patch then the re-enabled patch will show as properly scanned (either patched, not patched or not applicable depending on the device patch state of the original patch).

Although this is inconsistent with the behavior of earlier versions of Patch Management, this change is an improvement because only the patches that currently need to be installed are reported or analyzed on each device.

Action: None necessary.

Patch deployment might not start when scheduled

Source: ZENworks; Patch Management.

Possible Cause: If the deployment schedule type includes both the **Recurring** and **Process Immediately If the Device Is Unable to Execute** options, when the device becomes active, the deployment of the patch does not start on the first of its scheduled recurring dates. However, the patch is deployed when the next recurring date occurs.

Action: Instead of selecting a recurring schedule, select a date-specific schedule so that the patch is applied when the device becomes active.

Linux - Custom Patches: Bundles fail to launch

Source: ZENworks; Patch Management.

Possible Cause: RPM Application Bundle and Custom RPM Bundle fails on both SUSE as well as Red Hat when it is assigned to the device with Launch Schedule On Device Refresh.

Action: Work around for the custom patch: Add 1-2 minutes of delay execution after refresh for “Remediation Schedule” to resolve it.

Airgap Server: User receives trial license email after adding the license info to system variables

Source: ZENworks; Patch Management.

Explanation: After setting up an Airgap server, you receive trial license emails from the server although you’ve added your license to the Airgap server system variables.

Possible Cause: The Airgap server requires the Patch Management license file from the connected server.

Action: Contact Micro Focus Support.

Blank PowerShell window is displayed after deploying patch policies during device shutdown

Source: ZENworks; Patch Management.

Explanation: After assigning the Patch Policies on Shutdown schedule to a Windows 1903 device, during the device shutdown, a blank PowerShell window is displayed. Though the patches have installed correctly on the device, the Powershell window does not display any messages.

Action: None. Ignore the blank PowerShell window.

Unable to uninstall patches

Source: ZENworks; Patch Management.

Explanation: Patches that support uninstall cannot be removed from a device by clicking the Patched count within the Patches page in ZCC.

Action: To uninstall a patch, perform the following steps:

1. Go to Security > Patches.
2. Select a patch that can be installed.
3. On the left navigation menu, click View Patch.
4. Click the Patched tab.
5. Select a device, and then click Action > Remove.

Patch Policy assignment: Bundle stays in 'Pending' state forever

Source: ZENworks; Patch Management.

Possible Cause: There are issues between bundles and older agents

Action: Bundle Assignment having State as "Not Effective" has a reason associated like "System requirement failed", "Unsociable Type", "Blocked", "Wrong Platform" etc. Similarly we have to define a new State like "Not Effective because Older Agent" and then update the existing logic to set that State while filtering the assignments.

Adding / defining new State for Bundle Assignment has more impact as other components on server might be using the value of Effective State for other computations.

"Remediation cannot be deployed" error is displayed when remediating vulnerable devices from security dashboard

Explanation: When a patch is superseded and the managed device has not yet uploaded the status for the new patch, during this interval if you try to remediate the device, an error is displayed and inconsistency is seen in security dashlets. (Example, CVE Severity Distribution, Top CVEs, etc.)

Action: Wait for the patch status to update.

Configuration Issues

- "Deploying patches with Auto Reboot causes the device to shut down" on page 124

Deploying patches with Auto Reboot causes the device to shut down

Source: ZENworks 2017; Patch Management.

Possible Cause: Trying to deploy patches with auto-reboot might shut down the machine instead of rebooting. It might also fail to report patch results to the ZENworks Server.

Action: Perform reboots with a Quick Task rather than using the Auto Reboot option.

Error Codes

- "ERROR CODE: ERROR = 40" on page 126
- "ERROR CODE: PPX_ERROR_PATCH_MORE_THAN_MAXAPPLICABLE SIGS = 45" on page 126
- "ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2" on page 126
- "ERROR CODE: PPX_ERROR_PACKAGE_ARCHIVE_INITIALIZE = 8" on page 127
- "ERROR CODE: PPX_ERROR_EXTRACT_FILE = 20" on page 127
- "ERROR CODE: PPX_ERROR_PACKAGE_REIMPORT = 40" on page 127
- "ERROR CODE: PPX_ERROR_EXPIRED_LICENSE_KEY = 27" on page 127
- "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127
- "ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 3" on page 127
- "ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 4" on page 127
- "ERROR CODE: PPX_ERROR_PATCH_MANY_APPLICABLE_SIGNATURES = 5" on page 127
- "ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 6" on page 127
- "ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 7" on page 128
- "ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 9" on page 128
- "ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 10" on page 128
- "ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 11" on page 128
- "ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 12" on page 128
- "ERROR CODE: PPX_ERROR_SIGNATURE_PREREQ_CACHE_EXHAUSTED = 13" on page 128
- "ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 14" on page 128
- "ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 15" on page 128
- "ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_SYNTAX = 16" on page 128
- "ERROR CODE: PPX_ERROR_FINGERPRINT_FILEROOT_UNSUPPORTED = 17" on page 129
- "ERROR CODE: PPX_ERROR_FINGERPRINT_TYPE_UNSUPPORTED = 18" on page 129
- "ERROR CODE: PPX_ERROR_SCRIPT_BAD_FILEHANDLE = 19" on page 129
- "ERROR CODE: PPX_ERROR_WMI_FINGERPRINT_UNSUPPORTED = 22" on page 129
- "ERROR CODE: PPX_ERROR_JAVASCRIPT_UNSUPPORTED = 23" on page 129
- "ERROR CODE: PPX_ERROR_MISSING_PREREQ_SIGNATURE = 25" on page 129
- "ERROR CODE: PPX_ERROR_INVALID_PREREQ_LANGUAGE = 26" on page 129
- "ERROR CODE: PPX_ERROR_INVALID_ROOT_HKEY = 21" on page 129
- "ERROR CODE: PPX_ERROR_FINGERPRINT_INVALID_SYSINFO = 31" on page 129
- "ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_MISSING_VARIABLE = 32" on page 130
- "ERROR CODE: PPX_ERROR_FINGERPRINT_FILESCAN_UNSUPPORTED = 34" on page 130

- “ERROR CODE: PPX_ERROR_FINGERPRINT_WMI_ERROR = 35” on page 130
- “ERROR CODE: PPX_ERROR_RELEVANCE_SCRIPT_SYNTAX = 36” on page 130
- “ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41” on page 130
- “ERROR CODE: PPX_ERROR_ENTITLED_FILE_MISSING = 28” on page 130
- “ERROR CODE: PPX_ERROR_ENTITLED_FILE_BAD_CHECKSUM = 29” on page 130
- “ERROR CODE: PPX_ERROR_ENTITLED_FILE_WRONG_SIZE = 30” on page 130
- “ERROR CODE: PPX_ERROR_OUT_OF_MEMORY = 24” on page 131
- “ERROR CODE: PPX_ERROR_PACKAGE_MKDIR_FAILURE = 33” on page 131
- “ERROR CODE: PPX_ERROR_UNKNOWN” on page 131
- “ERROR CODE: 41” on page 131
- “ERROR CODE: 142” on page 131
- “ERROR CODE: 143” on page 131
- “ERROR CODE: 144” on page 132
- “ERROR CODE: 145” on page 132
- “ERROR MESSAGE: “There is an issue with checksum metadata at CDN”” on page 132
- “ERROR : zman prb "<baseline_patch_name>" - java.lang.NullPointerException when trying to get the DefaultHibernateSessionManager” on page 132
- “OTHER ERROR CODES” on page 133

ERROR CODE: ERROR = 40

Source: ZENworks 2017; Patch Management.

Possible Cause: The patch file cached to the ZCM Server is corrupt.

Action: Try re-caching the patch to the ZCM Server.

ERROR CODE: PPX_ERROR_PATCH_MORE_THAN_MAXAPPLICABLE SIGS = 45

Source: ZENworks 2017; Patch Management.

Possible Cause: The patch file contains more than the maximum applicable signatures.

Action: Notify Micro Focus Support of the error. We will fix the problem with the patch and notify you when it is fixed.

ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2

Source: ZENworks 2017; Patch Management.

Possible Cause: Extraction of the `.cab` file or its contents fails.

Action: Follow the steps below:

1. Make sure that CABARC runs on the end point where the error message appears.
2. Check the available disk space on the end point.

3 Re-cache the patch to the ZCM Server.

4 If the issue persists, contact Micro Focus Support.

ERROR CODE: PPX_ERROR_PACKAGE_ARCHIVE_INITIALIZE = 8

Source: See “ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 126.

ERROR CODE: PPX_ERROR_EXTRACT_FILE = 20

Source: See “ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 126.

ERROR CODE: PPX_ERROR_PACKAGE_REIMPORT = 40

Source: See “ERROR CODE: PPX_ERROR_ARCHIVE_EXTRACT = 2” on page 126.

ERROR CODE: PPX_ERROR_EXPIRED_LICENSE_KEY = 27

Source: ZENworks 2017; Patch Management.

Possible Cause: The `.plk` license file you are using is outdated or has expired. This error code might also appear if the license file is erased or did not get decrypted properly.

Action: Ensure that you have the latest System Update installed.

ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1

Source: ZENworks 2017; Patch Management.

Possible Cause: You might encounter any of these error codes if a patch has bad metadata.

Action: Contact Technical Support.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 3

Source: See “ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 127.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 4

Source: See “ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 127.

ERROR CODE: PPX_ERROR_PATCH_MANY_APPLICABLE_SIGNATURES = 5

Source: See “ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 127.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 6

Source: See “ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1” on page 127.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 7

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 9

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 10

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 11

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 12

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_SIGNATURE_PREREQ_CACHE_EXHAUSTED = 13

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_PATCH_OPEN_FAILURE = 14

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_PATCH_BAD_GUID = 15

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_SYNTAX = 16

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_FINGERPRINT_FILEROOT_UNSUPPORTED = 17

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_FINGERPRINT_TYPE_UNSUPPORTED = 18

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_SCRIPT_BAD_FILEHANDLE = 19

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_WMI_FINGERPRINT_UNSUPPORTED = 22

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_JAVASCRIPT_UNSUPPORTED = 23

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_MISSING_PREREQ_SIGNATURE = 25

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_INVALID_PREREQ_LANGUAGE = 26

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_INVALID_ROOT_HKEY = 21

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_FINGERPRINT_INVALID_SYSINFO = 31

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_FINGERPRINT_EXPRESSION_MISSING_VARIABLE = 32

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_FINGERPRINT_FILESCAN_UNSUPPORTED = 34

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_FINGERPRINT_WMI_ERROR = 35

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_RELEVANCE_SCRIPT_SYNTAX = 36

Source: See "ERROR CODE: PPX_ERROR_VARIABLE_CACHE_EXHAUSTED = 1" on page 127.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41

Source: ZENworks 2017; Patch Management.

Possible Cause: These error codes indicate possible problems in bundle distribution. The ZCM server might not be able to access a third-party website where bundles are located.

Action: Follow the steps below:

1. Check your Internet connection and firewall settings.
2. Check that the ZCM Server can access a third-party website such as the Microsoft Download Center (http://www.microsoft.com/downloads/en/default.aspx).
3. Download patches from the third-party website.
4. Re-cache the downloaded patches.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_MISSING = 28

Source: See "ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41" on page 130.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_BAD_CHECKSUM = 29

Source: See "ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41" on page 130.

ERROR CODE: PPX_ERROR_ENTITLED_FILE_WRONG_SIZE = 30

Source: See "ERROR CODE: PPX_ERROR_ENTITLED_FILE_INVALID = 41" on page 130.

ERROR CODE: PPX_ERROR_OUT_OF_MEMORY = 24

Source: ZENworks 2017; Patch Management.

Possible Cause: This error arises when there is a deficiency in system resources, such as insufficient disk space, low available memory, and so on.

Action: Check the available disk space and memory, then verify that it is sufficient to meet the ZCM Server and Agent requirements.

ERROR CODE: PPX_ERROR_PACKAGE_MKDIR_FAILURE = 33

Source: ZENworks 2017; Patch Management.

Possible Cause: The user has insufficient permissions to carry out the specified action.

Action: Check whether you have appropriate system rights or permissions.

ERROR CODE: PPX_ERROR_UNKNOWN

Source: ZENworks 2017; Patch Management.

Possible Cause: This error is a a general exception. If logging is enabled, the error is recorded in the `.log` file.

Action: Follow the steps below:

1. Open a support ticket with Lumension.
2. Contact Micro Focus Support.

ERROR CODE: 41

Source: ZENworks 2017; Patch Management.

Possible Cause: This error code implies that ZENworks Patch Management was unable to perform patch remediation. This error occurs when deployment of a different version of the same patch is in progress.

Action: Wait for the previous deployment to complete, then deploy the patch again.

ERROR CODE: 142

Source: ZENworks 2017; Patch Management.

Possible Cause: The selected patch requires certain prerequisites before the patch can be deployed. This error can also occur when package files for a patch are unavailable.

Action: Contact Micro Focus Support and report the patch name. This is most likely a bad patch.

ERROR CODE: 143

Source: ZENworks 2017; Patch Management.

Possible Cause: This error is a a general exception. If logging is enabled, the error is recorded in the `.log` file.

Action: Follow the steps below:

1. Redeploy the patch.
2. If the error persists, file an incident report with Micro Focus.

ERROR CODE: 144

Source: ZENworks 2017; Patch Management.

Possible Cause: This error code appears if there are errors in the patch deployment script. If logging is enabled, the error is recorded in the `.log` file.

Action: File an incident report with Micro Focus.

ERROR CODE: 145

Source: ZENworks 2017; Patch Management.

Possible Cause: The script failed to open the registry. This issue is most probably associated with timing.

Action: Deploy the patch again.

ERROR MESSAGE: “There is an issue with checksum metadata at CDN”

Source: ZENworks 2017; Patch Management.

Possible Cause: There is a problem with not having access to the VEGA content path.

Action: Check the following URL’s and see if you can download them:

http://cache.patchlinksecure.net/PatchComponents/OSPXSet.xml

http://cache.lumension.com/patchcomponents/1f12ad89-5711-41ce-ae84-9df6487153f3/win8x64.ospx

ERROR : zman prb "<baseline_patch_name>" - java.lang.NullPointerException when trying to get the DefaultHibernateSessionManager

Source: ZENworks 2017; Patch Management.

Possible Cause: zman prb "<baseline_patch_name>" is throwing a java.lang.NullPointerException.This is being caused by code returning a null DefaultHibernateSessionManager.

The following error will be seen:.

Code:
com.novell.zenworks.zman.commands.PatchHandler.patchRemoveBaseline()Line: 123 DirectServiceStoreImpl dssi = (DirectServiceStoreImpl) store;Line: 124 DefaultHibernateSessionManager dsm =(DefaultHibernateSessionManager)

((HibernateAbstractSession)dssi.getSession()).getSessionManager();Line: 125 session = dsm.openSession();StackTrace:java.lang.NullPointerException (java.lang.StackTraceElement[])[com.novell.zenworks.zman.commands.PatchHandler.patchRemoveBaseline(PatchHandler.java:125),sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method),sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57),sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43),java.lang.reflect.Method.invoke(Method.java:606),com.novell.zenworks.zman.CommandRunner.execute(CommandRunner.java:94),com.novell.zenworks.zman.ZMan.executeRunner(ZMan.java:328),com.novell.zenworks.zman.ZMan.runCommand(ZMan.java:531),com.novell.zenworks.zman.ZMan.main(ZMan.java:465),com.novell.zenworks.zman.ZManExecutor.execute(ZManExecutor.java:101),com.novell.zenworks.zman.ZManExecutor.main(ZManExecutor.java:41),sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method),sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57),sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43),java.lang.reflect.Method.invoke(Method.java:606),com.novell.zenworks.zman.ZManLoader.loadZMan(ZManLoader.java:59),com.novell.zenworks.zman.ZManLoader.main(ZManLoader.java:143)]

Action: Increase memory size as follows:

modify "JVM_STARTUP_OPTIONS=-Xms64m -Xmx128m" to"JVM_STARTUP_OPTIONS=-Xms64m -Xmx1024m" in the zman-config.properties file. The error disappears and indicates the baseline clears successfully.

Then,

1. Assign a baseline in a group.
2. Refresh the agent to receive the baseline.
3. Remove the baseline on the server.
4. Refresh agent again and notice the baseline should remain.
5. Modify memory in the file "zman-config.properties file."
6. Refresh the agent again.

OTHER ERROR CODES

Source: ZENworks 2017; Patch Management.

Action: Contact Micro Focus Support.

B System Variables

Within ZENworks Control Center, you can enter system variables to enable or disable certain Patch Management behaviors.

Patch Management System Variables

Patch Management System Variables

See below for a list of variables and how to enter them. You can enter these variables by selecting **Configuration** > **Configuration** page > **Device Management** > **System Variables**.

NOTE: All system variables are case-sensitive.

---

zpm-log-retain-days

Set how long the files in the folders specified by the zpm-folders-to-clean setting should be retained on the managed device. The default value is 7 days, which means that any files older than 7 days will be removed from the specified folders.

zpm-folders-to-clean

The ZPM folder contains three subfolders: logs, stage, and content. By default, each folder is cleaned up after the number of days specified by the zpm-log-retain-days variable. Use this variable to limit which folders are cleaned up. For example, if you only want the stage and content folders to be cleaned up, specify only these two folders. Any folder not specified will not be cleaned up. Separate folder entries with a comma.

In general, it is recommended that you clean up all three folders so that excess disk space is not consumed. This variable is typically used only in conjunction with OpenText Customer Care when troubleshooting issues.

zpm-clean-up-timer

Set the interval period for the folder cleanup. The default value is 12, which means that every 12 hours any files older than the zpm-log-retain-days setting will be deleted from the folders specified by the zpm-folders-to-clean setting.

AIRGAP_COLLECTOR_ALWAYS_DOWNLOAD

Set to `true` to force to download all bundles and expected patches on the Airgap connection server.

(For troubleshooting only)

CONNECTION_TIMEOUT

Enables the adjustment of URL connection timeout duration when downloading patch files (signatures, packages & payloads). Using this system variable can be beneficial when operating in a slow or intermittent network environment.

Default Value: 180 seconds

Valid Range: 0 (infinite) to 3600 seconds (1 hour)

PATCH_AIRGAP_COLLECTOR

Set to `true` to enable Airgap function on the connection server.

PATCH_AIRGAP_LICENSE

Set valid license for the Airgap disconnection server.

PATCH_AIRGAP_SERVER

Set to `true` to enable Airgap function on the disconnection server.

PATCH_ALWAYS_SHOW_REBOOT_PROMPT

Set to `true` to display the patch reboot prompt to users when the Patch Policy Reboot Behavior option for **Suppress reboot** is set to **Yes**.

No prompt is displayed on **Suppress reboot** if this variable is set to `false`, which is the default behavior.

PATCH_CONVERT_BASELINES_TO_POLICIES

Set to `false` to skip the process of converting mandatory baselines to patch policies.

PATCH_DAU_SYSTEM_CONTENT

If that is set to `true` then DAU bundles are created with content type of Patch System.

NOTE: If this is not set prior to existing DAU bundles being created, it is necessary to delete the existing DAU bundles and then run the Patch Server maintenance update.

Default Value: `false`

Valid Values: `true, false`

PATCH_DELAY_REBOOT_ANALYZE

Delays the initial patch scan, which is run during device startup, by the specified number of minutes, when a reboot-required patch is installed and the system is rebooted

Valid Range: From 1 to 60 minutes. If the specified value is above 60, then the Analyze process will be delayed by 60 minutes.

Value: Integer value in minutes (from 1 to 60).

PATCH_DELAY_SUPERSEDED_DISABLE

Delays the disabling of superseded patches by the specified number of days. The value configured using this system variable will override the value configured in ZENworks Control Center.

Default Value: 120 days

PATCH_DEPLOY_USER_SYSTEM

Set true or false to specify the Window executable's security level.

`true`: The option **Run as secure system user (Don't allow system to interact with desktop)** will be selected.

`false`: The option **Run as dynamic administrator** will be selected.

PATCH_NOTIFY_INSTALL_ALLOWCANCEL

Set to `true` to allow the user to cancel the patch installation.

PATCH_NOTIFY_INSTALL_POPUP_DURATION

Set value to define how long the system tray notification is displayed before being hidden.

PATCH_NOTIFY_INSTALL_POPUP_SHOW_TRAY

Set to `true` to enable a notification for a pending installation is displayed in the system tray.

PATCH_NOTIFY_INSTALL_MESSAGE

Set value for the text of the notification message.

PATCH_NOTIFY_INSTALL_MESSAGE_POPUP

Set value for text that appears in the notification.

PATCH_NOTIFY_INSTALL_NOTIFYUSER

Set to `true` to notify the user prior to the installation of the patch.

PATCH_NOTIFY_INSTALL_REBOOT_TIMEOUT

Set the value of the countdown for install notification.

PATCH_NOTIFY_INSTALL_SNOOZE

Set to `true` to allow the user to delay the installation.

PATCH_NOTIFY_INSTALL_SNOOZE_INTERVAL

Set the value for the duration the install is delayed when the user snoozes.

PATCH_NOTIFY_REBOOT_ALLOWCANCEL

Set to `true` to enable a cancel option in the reboot notification prompt.

PATCH_NOTIFY_REBOOT_MESSAGE

Set value for the text of the message that appears before patch installation completes and the computer reboots.

PATCH_NOTIFY_REBOOT_MESSAGE_POPUP

Set value for text that appears in the notification.

PATCH_NOTIFY_REBOOT_NOTIFYUSER

Set to `true` to enable reboot notification and its configuration options.

PATCH_NOTIFY_REBOOT_POPUP_DURATION

Enter a value in hours, minutes or seconds for how long the system tray notification is displayed before being hidden.

PATCH_NOTIFY_REBOOT_POPUP_SHOW_TRAY

Set to `true` to enable a notification for a pending reboot which is displayed in the system tray.

PATCH_NOTIFY_REBOOT_REBOOT_TIMEOUT

Set the value of the countdown for reboot notification.

PATCH_NOTIFY_REBOOT_SNOOZE

Set to `true` to enable a snooze option in the deployment reboot notification prompt, which delays the reboot.

PATCH_NOTIFY_REBOOT_SNOOZE_INTERVAL

Set the value for the duration the reboot is delayed when the user clicks **Snooze**.

PATCH_NOTIFY_REBOOT_SUPPRESSREBOOT

Set to `true` to enable an option in the reboot notification prompts to prevent the reboot.

PATCH_POLICY_ACTIONS_LIMIT

Enables adjustments of the maximum number of patch policy actions. Thus, using this system variable allows users finer control of patch policy child bundle actions.

Default Value: 1500 actions

Valid Range: 100 to 99999 actions

PATCH_SCAN_ALWAYS

Set to `true` to ensure that the patch detection scan runs on all devices as scheduled, even when patch discovery for new content does not indicate the need for a scan. When the variable is not set, the default behavior is the same as `true`.

Default Value: `true`

Valid Values: `true, false`

PATCH_TREND_DATA_DAYS

This variable controls the number of days that patch Dashboard and Trending data, which was configured in an earlier version of ZENworks, is stored in the database. Set the value to `x` days of storing data or set it to `0` to disable storing the data.

NOTE: Patch Dashboard and Trending provided patch compliance and trending data on the Patch dashboard in ZENworks 2017 Update 2 and earlier versions. This variable is only applicable to ZENworks Patch Management environments that have updated to ZENworks Patch Management 2017 Update 4 from an earlier version. It is not applicable for new installations from Update 4 and later. For information about accessing this data, contact Technical Support.

---

scan.software.installers

This variable, when set to `true`, enables ZENworks Patch Management to manage applicable Windows Software Installers. For example, Microsoft 365 apps patching. For more information, see Enabling Software Installers.

Default Value: `false`

Valid Values: `true`, `false`

PATCH_SIZE_LIMIT_FOR_CURL

Set the value above which the patch should be downloaded using cURL. Specify the size in MB. By default, the patch download limit size is 1024 MB.

PATCH_CUSTOM_DOWNLOAD_PATH

Set a custom path to the cURL configuration to the downloaded patch file path (without file name) for a custom patch.

USE_CURL_ON_CUSTOM_DOWNLOAD_FAILURE: In case the custom file does not have the required path, in such cases this variable can be set to true so that the patches can be downloaded from the default location. This variable cannot be used independently.

The above two variables should be used together. By default, USE_CURL_ON_CUSTOM_DOWNLOAD_FAILURE is set to false.

CURL_CONFIG_PATH

Set the path to the cURL configuration with the file name.

If you are using a proxy, then ensure that you add the following parameters in the configuration file:

- dump-header="curl-response-headers.log"
- proto=https
- proxy=<proxy_address>:7443

REMEDIATOR_PASSWORD_MINIMUM_LENGTH

Set minimum password length for Remediator user.

REMEDIATOR_PASSWORD_MAXIMUM_LENGTH

Set maximum password length for Remediator user.

NOTE: Both *REMEDIATOR_PASSWORD_MAXIMUM_LENGTH* and *REMEDIATOR_PASSWORD_MINIMUM_LENGTH* should be configured, even if one variable is not configured, then by default, the minimum and maximum password length will be 10 and 15 respectively.

REMEDIATION_USER_PASSWORD_TTL

Set Time To Live for remediation User Password. By default, TTL is set to 7 days.

MACOS_PATCH_DOWNLOAD_URL_DOMAIN_NAME

Set the fragment of the download URL for the Mac OS patch, if apple.com is not part of the patch URL.

By default, this system variable is resolved to apple.com, if not configured. Describes a fragment of Mac OS patch download URL, if apple.com is not a part of the patch URL.

AIRGAP_SERVER

Set to true when the zone is an Airgap server.

AIRGAP_COLLECTOR

Set to true when the zone is Airgap collector.

useSysVarLocale

Set to true to the use LANG_CODE variable.

LANG_CODE

Specify the language code from the language catalog. For example, en-US

MACOS_PATCH_DOWNLOAD_URL_DOMAIN_NAME

Specify a fragment of the download URL from where patch will be downloaded.